

BEST AVAILABLE COPY

REC'D 15 APR 2004

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

WIPO PCT

PCT/JP 2004/004338

26. 3. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日      2 0 0 3 年    3 月 2 8 日  
Date of Application:

出 願 番 号      特 願 2 0 0 3 - 0 9 2 6 4 7  
Application Number:  
[ST. 10/C]:      [ J P 2 0 0 3 - 0 9 2 6 4 7 ]

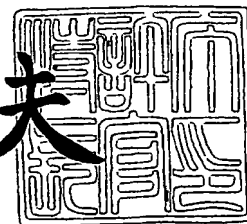
出    願    人      ソニー株式会社  
Applicant(s):

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 3 年 1 2 月    8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 3 - 3 1 0 1 4 8 0

【書類名】 特許願

【整理番号】 0390209013

【提出日】 平成15年 3月28日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/46

【発明者】

【住所又は居所】 東京都品川区北品川 6丁目 7番 35号 ソニー株式会社  
内

【氏名】 板橋 達夫

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理システム、情報処理装置および情報処理方法、記録媒体、並びにプログラム

【特許請求の範囲】

【請求項 1】 ユーザにより操作される端末と、  
リソースを提供する第 1 の親機と、  
前記ユーザの個人情報を記憶する第 2 の親機と、  
電子バリューを管理するバリュー装置と  
を備える情報処理システムにおいて、  
前記端末は、

前記第 1 の親機が提供するリソースを要求する信号を、前記第 2 の親機に送信するリソース要求信号送信手段と、

前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する第 1 の利用権取得手段と

を有し、

前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用し、

前記第 1 の親機は、

前記リソースの提供に対する対価としての電子バリューが、前記第 2 の親機から前記第 1 の親機に振り込まれたことの振込み通知を、前記バリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記第 2 の親機に対して、前記利用権を発行する利用権発行手段と

を有し、

前記端末が、前記利用権を提示した場合に、自身が有するリソースの利用を許可し、

前記第 2 の親機は、

前記端末装置から送信されてくる、前記リソースを要求する信号に応じて、前記第 1 の親機への前記電子バリューの振込みを、前記バリュー装置に要求する

電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記第1の親機が発行する前記利用権を取得する第2の利用権取得手段と、

前記第2の利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段と

を有し、

前記バリュー装置は、

前記第2の親機からの要求に応じて、前記第1の親機に前記電子バリューを振り込む電子バリュー振込み手段と、

前記第1の親機への前記電子バリューの振込み通知を、前記第1の親機に送信する振込み通知送信手段と

を有する

ことを特徴とする情報処理システム。

【請求項2】 ユーザにより操作される情報処理装置において、

リソースを提供する第1の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信手段と、

前記第1の親機が提供するリソースを利用する利用権を、前記第2の親機から取得する利用権取得手段と

を備え、

前記利用権を、前記第1の親機に提示して、前記第1の親機が提供するリソースを利用する

ことを特徴とする情報処理装置。

【請求項3】 前記第2の親機との間で、前記ユーザが前記第2の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備える

ことを特徴とする請求項2に記載の情報処理装置。

【請求項4】 前記リソース要求信号送信手段と前記利用権取得手段は、前記第1の親機を介して、前記第2の親機とやりとりする

ことを特徴とする請求項2に記載の情報処理装置。

【請求項 5】 前記リソース要求信号送信手段と前記利用権取得手段は、前記第 2 の親機との間で、データを暗号化してやりとりする

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 6】 前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 7】 ユーザにより操作される情報処理装置の情報処理方法において、

リソースを提供する第 1 の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第 2 の親機に送信するリソース要求信号送信ステップと、

前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用する

ことを特徴とする情報処理方法。

【請求項 8】 ユーザにより操作される情報処理装置に実行させるプログラムであって、

リソースを提供する第 1 の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第 2 の親機に送信するリソース要求信号送信ステップと、

前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用する

ことを特徴とするプログラム。

【請求項 9】 ユーザにより操作される端末に、自身が有するリソースを提

供する情報処理装置において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段と

を備え、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理装置。

【請求項 10】 前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項 9 に記載の情報処理装置。

【請求項 11】 前記振込み通知が正当であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項 9 に記載の情報処理装置。

【請求項 12】 前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項 9 に記載の情報処理装置。

【請求項 13】 ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置の情報処理方法において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理方法。

【請求項 14】 ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置に実行させるプログラムであって、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とするプログラム。

【請求項 15】 ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段と、

前記利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段と

を備えることを特徴とする情報処理装置。

【請求項 16】 前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項 15 に記載の情報処理装置。

【請求項 17】 前記端末との間で、前記ユーザが前記個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備える

ことを特徴とする請求項 15 に記載の情報処理装置。

【請求項 18】 前記リソースは、装置、情報、または情報に対するライセンス

ンスである

ことを特徴とする請求項 15 に記載の情報処理装置。

【請求項 19】 ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置の情報処理方法において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とする情報処理方法。

【請求項 20】 ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置に実行させるプログラムにおいて、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とするプログラム。

【請求項 21】 電子バリューを管理する情報処理装置において、

ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第 2 の親機からの要求に応じて行う電子バリュー振込み手段と

、  
前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信手段と



を備えることを特徴とする情報処理装置。

【請求項 22】 前記第 1 または第 2 の親機との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えることを特徴とする請求項 21 に記載の情報処理装置。

【請求項 23】 前記第 1 と第 2 の親機の電子バリューを記憶する記憶手段をさらに備え、

前記電子バリュー振込み手段は、前記記憶手段に記憶された電子バリューを書き換えることにより、前記第 2 の親機から前記第 1 の親機に対して、前記電子バリューを振り込む

ことを特徴とする請求項 21 に記載の情報処理装置。

【請求項 24】 前記電子バリュー振込み手段は、前記第 2 の親機から電子バリューを取得し、その電子バリューを前記第 1 の親機に送信することにより、前記第 2 の親機から前記第 1 の親機に対して、前記電子バリューを振り込む

ことを特徴とする請求項 21 に記載の情報処理装置。

【請求項 25】 前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項 21 に記載の情報処理装置。

【請求項 26】 電子バリューを管理する情報処理装置の情報処理方法において、

ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報記憶する第 2 の親機からの要求に応じて行う電子バリュー振込みステップと、

前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信ステップとを含むことを特徴とする情報処理方法。

【請求項 27】 電子バリューを管理する情報処理装置に実行させるプログラムであって、

ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、その

リソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報記憶する第2の親機からの要求に応じて行う電子バリュー振込みステップと、

前記第2の親機から前記第1の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第1の親機に送信する振込み通知送信ステップとを含むことを特徴とするプログラム。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、情報処理システム、情報処理装置および情報処理方法、記録媒体、並びにプログラムに関し、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のままユーザの嗜好に合わせた操作性で操作させることができるようにした情報処理システム、情報処理装置および情報処理方法、記録媒体、並びにプログラムに関する。

##### 【0002】

#### 【従来の技術】

近年、携帯型のパーソナルコンピュータ、携帯電話などが普及し、多くのユーザがこれら通信機能、情報処理機能を有する小型の装置を携帯し、屋外で、あるいは移動先においてネットワークに接続してネットワークを介する通信を行っている。

##### 【0003】

ここで、既存のインフラを利用したシステムとして、すでに存在する様々な通信網を適宜切り替えて利用するパーソナル通信サービス分散システムが提案されている（例えば特許文献1）。このシステムは、例えば電子メールサービスや電話サービス等の異なるネットワーク通信網を統合して利用することを可能としたシステムである。

##### 【0004】

しかしながら、ユーザが外出中のような状況で、出先に有るたまたま身近な機器を、自らの所有する同種機種と同じ感覚で利用することはセキュリティやプラ

イバシ等の問題があり、実現されていなかった。

【0005】

【特許文献1】

特開平8-56263号公報

【0006】

【発明が解決しようとする課題】

そこで、ユーザが匿名のまま、他者に所有管理されるリソースを所有者との間で相互の信頼関係に基づくセッションを構築し、その上で自らの管理する嗜好情報にしたがって制御することが提案されている。

【0007】

しかしながら、この方法では、一方的に他者のリソースを使い続けるユーザや、他者のリソースを使う機会が少ないにもかかわらず、自ら所有するリソースを提供し続けるユーザがいる場合、需給のバランスがとれなくなる恐れがある。

【0008】

そこで、ユーザが、他者の所有するリソースを利用するために必要な対価を、自分と他者の対価を管理する装置を介して支払うシステムが提案されている。

【0009】

このとき、ユーザが対価を管理する装置と直接アクセスすることによって、ユーザの匿名性を確保することが考えられる。

【0010】

しかしながら、ここで確保されるユーザの匿名性は、利用シーン（リソースを利用しているとき）の匿名性だけであり、ユーザの個人情報是对価を管理する装置に管理される。従って、ユーザが匿名のまま対価を支払い、他者の所有するリソースを利用することは困難であった。

【0011】

また、対価を前提に公共の場で通信サービスを行っている無線LAN (Local Area Network) 等の事業者とのシームレスなサービスをユーザに提供することは困難であった。

【0012】

本発明は、このような状況に鑑みてなされたものであり、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作することができるようにするものである。

### 【0013】

#### 【課題を解決するための手段】

本発明の情報処理システムは、ユーザにより操作される端末と、リソースを提供する第1の親機と、ユーザの個人情報を記憶する第2の親機と、電子バリューを管理するバリュー装置とを備える情報処理システムであって、端末は、第1の親機が提供するリソースを要求する信号を、第2の親機に送信するリソース要求信号送信手段と、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する第1の利用権取得手段とを有し、利用権を、第1の親機に提示して、第1の親機が提供するリソースを利用し、第1の親機は、リソースの提供に対する対価としての電子バリューが、第2の親機から第1の親機に振り込まれたことの振込み通知を、バリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、第2の親機に対して、利用権を発行する利用権発行手段とを有し、端末が、利用権を提示した場合に、自身が有するリソースの利用を許可し、第2の親機は、端末装置から送信されてくる、リソースを要求する信号に応じて、第1の親機への電子バリューの振込みを、バリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、第1の親機が発行する利用権を取得する第2の利用権取得手段と、第2の利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを有し、バリュー装置は、第2の親機からの要求に応じて、第1の親機に電子バリューを振り込む電子バリュー振込み手段と、第1の親機への電子バリューの振込み通知を、第1の親機に送信する振込み通知送信手段とを有することを特徴とする。

### 【0014】

本発明の第1の情報処理装置は、リソースを提供する第1の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信手段と、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する利用権取得手段とを備え、利用権を、第1の親機に提

示して、第1の親機が提供するリソースを利用することを特徴とする。

【0015】

第2の親機との間で、ユーザが第2の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

【0016】

リソース要求信号送信手段と利用権取得手段は、第1の親機を介して、第2の親機とやりとりするようにすることができる。

【0017】

リソース要求信号送信手段と利用権取得手段は、第2の親機との間で、データを暗号化してやりとりするようにすることができる。

【0018】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【0019】

本発明の第1の情報処理装置の情報処理方法は、リソースを提供する第1の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信ステップと、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する利用権取得ステップとを含み、利用権を、第1の親機に提示して、第1の親機が提供するリソースを利用することを特徴とする。

【0020】

本発明の第1の情報処理装置のプログラムは、リソースを提供する第1の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信ステップと、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する利用権取得ステップとを含み、利用権を、第1の親機に提示して、第1の親機が提供するリソースを利用することを特徴とする。

【0021】

本発明の第2の情報処理装置は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段とを備え、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

#### 【0022】

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

#### 【0023】

振込み通知が正当であることの認証を行う認証手段をさらに備えるようにすることができる。

#### 【0024】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

#### 【0025】

本発明の第2の情報処理装置の情報処理方法は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

#### 【0026】

本発明の第2の情報処理装置のプログラムは、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得

した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

#### 【0027】

本発明の第3の情報処理装置は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段と、利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを備えることを特徴とする。

#### 【0028】

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

#### 【0029】

端末との間で、ユーザが個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

#### 【0030】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

#### 【0031】

本発明の第3の情報処理装置の情報処理方法は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。

#### 【0032】

本発明の第3の情報処理装置のプログラムは、端末からの要求に応じて、端末

にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。

#### 【0033】

本発明の第4の情報処理装置は、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込み手段と、第2の親機から第1の親機への電子バリューの振込みが行われたことを表す振込み通知を、第1の親機に送信する振込み通知送信手段とを備えることを特徴とする。

#### 【0034】

第1または第2の親機との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

#### 【0035】

第1と第2の親機の電子バリューを記憶する記憶手段をさらに備え、電子バリュー振込み手段は、記憶手段に記憶された電子バリューを書き換えることにより、第2の親機から第1の親機に対して、電子バリューを振り込むようにすることができる。

#### 【0036】

電子バリュー振込み手段は、第2の親機から電子バリューを取得し、その電子バリューを第1の親機に送信することにより、第2の親機から第1の親機に対して、電子バリューを振り込むようにすることができる。

#### 【0037】

本発明の第4の情報処理装置の情報処理方法は、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第2の親機からの



要求に応じて行う電子バリュー振込みステップと、第2の親機から第1の親機への電子バリューの振込みが行われたことを表す振込み通知を、第1の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

#### 【0038】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

#### 【0039】

本発明の第4の情報処理装置のプログラムは、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込みステップと、第2の親機から第1の親機への電子バリューの振込みが行われたことを表す振込み通知を、第1の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

#### 【0040】

本発明においては、端末により、第1の親機が提供するリソースを要求する信号が、第2の親機に送信され、記第1の親機が提供するリソースを利用する利用権が、第2の親機から取得される。そして、利用権が、第1の親機に提示され、第1の親機が提供するリソースが利用される。また、第1の親機により、リソースの提供に対する対価としての電子バリューが、第2の親機から第1の親機に振り込まれたことの振込み通知が、バリュー装置から受信され、振込み通知に応じて、第2の親機に対して、利用権が発行される。また、第1の親機により、端末により利用権が提示された場合に、自身が有するリソースの利用が許可される。第2の親機により、端末装置から送信されてくる、リソースを要求する信号に応じて、第1の親機への電子バリューの振込みが、バリュー装置に要求され、電子バリューの振込みに応じて、第1の親機が発行する利用権が取得される。また、第2の親機により、取得された利用権が、端末に提供される。バリュー装置により、第2の親機からの要求に応じて、第1の親機に電子バリューが振り込まれ、第1の親機への電子バリューの振込み通知が、第1の親機に送信される。

#### 【0041】

**【発明の実施の形態】**

以下に本発明の実施の形態を説明するが、請求項に記載の構成要件と、発明の実施の形態における具体例との対応関係を例示すると、次のようになる。この記載は、請求項に記載されている発明をサポートする具体例が、発明の実施の形態に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、構成要件に対応するものとして、ここには記載されていない具体例があったとしても、そのことは、その具体例が、その構成要件に対応するものではないことを意味するものではない。逆に、具体例が構成要件に対応するものとしてここに記載されていたとしても、そのことは、その具体例が、その構成要件以外の構成要件には対応しないものであることを意味するものでもない。

**【0042】**

さらに、この記載は、発明の実施の形態に記載されている具体例に対応する発明が、請求項に全て記載されていることを意味するものではない。換言すれば、この記載は、発明の実施の形態に記載されている具体例に対応する発明であって、この出願の請求項には記載されていない発明の存在、すなわち、将来、分割出願されたり、補正により追加される発明の存在を否定するものではない。

**【0043】**

請求項1に記載の情報処理システムは、ユーザにより操作される端末（例えば、図1の移動端末装置11-2）と、リソースを提供する第1の親機（例えば、図1の親機12-1）と、前記ユーザの個人情報を記憶する第2の親機（例えば、図1の親機12-2）と、電子バリューを管理するバリュー装置（例えば、図1のバリュー発行装置14）とを備え、前記端末は、前記第1の親機が提供するリソースを要求する信号を、前記第2の親機に送信するリソース要求信号送信手段（例えば、図19のステップS209の処理を実行するCPU61）と、前記第1の親機が提供するリソースを利用する利用権（例えば、リソース利用権）を、前記第2の親機から取得する第1の利用権取得手段（例えば、図19のステップS210の処理を実行するCPU61）とを有し、前記利用権を、前記第1の親機に提示して、前記第1の親機が提供するリソースを利用し（例えば、図19のス

トップ S 2 1 1, S 2 1 2 の処理を実行する CPU 6 1)、前記第 1 の親機は、前記リソースの提供に対する対価としての電子バリューが、前記第 2 の親機から前記第 1 の親機に振り込まれたことの振込み通知を、前記バリュー装置から受信する振込み通知受信手段(例えば、図 1 9 のステップ S 2 6 5 の処理を実行する親機 1 2-1 の CPU 1 1 1)と、前記振込み通知に応じて、前記第 2 の親機に対して、前記利用権を発行する利用権発行手段(例えば、図 1 9 のステップ S 2 6 8 の処理を実行する親機 1 2-1 の CPU 1 1 1)とを有し、前記端末が、前記利用権を提示した場合に、自身が有するリソースの利用を許可し(例えば、図 9 のステップ S 8 3, S 8 4 の処理)、前記第 2 の親機は、前記端末装置から送信されてくる、前記リソースを要求する信号に応じて、前記第 1 の親機への前記電子バリューの振込みを、前記バリュー装置に要求する電子バリュー振込み要求手段(例えば、図 1 9 のステップ S 3 1 8 の処理を実行する親機 1 2-2 の CPU 1 1 1)と、前記電子バリューの振込みに応じて、前記第 1 の親機が発行する前記利用権を取得する第 2 の利用権取得手段(例えば、図 1 9 のステップ S 3 2 1 の処理を実行する親機 1 2-2 の CPU 1 1 1)と、前記第 2 の利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段(例えば、図 1 9 のステップ S 3 2 4 の処理を実行する親機 1 2-2 の CPU 1 1 1)とを有し、前記バリュー装置は、前記第 2 の親機からの要求に応じて、前記第 1 の親機に前記電子バリューを振り込む電子バリュー振込み手段(例えば、図 1 6 のステップ S 1 6 7 の処理を実行するバリュー発行部 1 3 5)と、前記第 1 の親機への前記電子バリューの振込み通知を、前記第 1 の親機に送信する振込み通知送信手段(例えば、図 1 9 のステップ S 3 4 4 の処理を実行するバリュー発行部 1 3 5)とを有することを特徴とする。

#### 【0044】

請求項 2 に記載の情報処理装置は、リソースを提供する第 1 の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第 2 の親機に送信するリソース要求信号送信手段(例えば、図 1 9 のステップ S 2 0 9 の処理を実行する CPU 6 1)と、前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する利用権取得手段(例えば、図 1 9 のステップ S 2 1

0 の処理を実行する CPU 61) とを備え、前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用する (図 19 のステップ S 211, S 212 の処理) ことを特徴とする。

#### 【0045】

前記第 2 の親機との間で、前記ユーザが前記第 2 の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段 (例えば、図 19 のステップ S 205 乃至ステップ S 208 の処理を実行する CPU 61) をさらに備えるようにすることができる。

#### 【0046】

前記リソース要求信号送信手段と前記利用権取得手段は、前記第 1 の親機を介して、前記第 2 の親機とやりとりするようにすることができる。

#### 【0047】

前記リソース要求信号送信手段と前記利用権取得手段は、前記第 2 の親機との間で、データを暗号化してやりとりするようにすることができる。

#### 【0048】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

#### 【0049】

請求項 7 に記載の情報処理方法、および請求項 8 に記載のプログラムは、リソースを提供する第 1 の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第 2 の親機に送信するリソース要求信号送信ステップ (例えば、図 19 のステップ S 209) と、前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する利用権取得ステップ (例えば、図 19 のステップ S 210) とを含み、前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用する (図 19 のステップ S 211, S 212 の処理) ことを特徴とする。

#### 【0050】

請求項 9 に記載の情報処理装置は、前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの

振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段（例えば、図19のステップS265の処理を実行する親機12-1のCPU111）と、前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段（例えば、図19のステップS268の処理を実行する親機12-1のCPU111）とを備え、前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する（例えば、図9のステップS83、S84の処理）ことを特徴とする。

#### 【0051】

前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

#### 【0052】

前記振込み通知が正当であることの認証を行う認証手段（例えば、図19のステップS266、S267の処理を実行する親機12-1のCPU111）をさらに備えるようにすることができる。

#### 【0053】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

#### 【0054】

請求項13に記載の情報処理方法、請求項11に記載の記録媒体、および請求項14に記載のプログラムは、前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップ（例えば、図19のステップS265）と、前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップ（例えば、図19のステップS268）とを含み、前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する（例えば、図9のステップS83、S84の処理）ことを特徴とする。

#### 【0055】

請求項 15 に記載の情報処理装置は、前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段（例えば、図 19 のステップ S 318 の処理を実行する親機 12-2 の CPU 111）と、前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段（例えば、図 19 のステップ S 321 の処理を実行する親機 12-2 の CPU 111）と、前記利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段（例えば、図 19 のステップ S 324 の処理を実行する親機 12-2 の CPU 111）とを備えることを特徴とする。

#### 【0056】

前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段（例えば、図 19 のステップ S 319, S 320 の処理を実行する親機 12-2 の CPU 111）をさらに備えるようにすることができる。

#### 【0057】

前記端末との間で、前記ユーザが前記個人情報に対応する正当なユーザであることの認証を行う認証手段（例えば、図 19 のステップ S 311 乃至ステップ S 314 の処理を実行する親機 12-2 の CPU 111）をさらに備えるようにすることができる。

#### 【0058】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

#### 【0059】

請求項 19 に記載の情報処理方法、および請求項 20 に記載のプログラムは、前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップ（例えば、図 19 のステップ S 318）と、前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステ

ップ（例えば、図19のステップS321）と、前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップ（例えば、図19のステップS324）とを含むことを特徴とする。

#### 【0060】

請求項21に記載の情報処理装置は、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込み手段（例えば、図16のステップS167の処理を実行するバリュー発行部135）と、前記第2の親機から前記第1の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第1の親機に送信する振込み通知送信手段（例えば、図19のステップS344の処理を実行するバリュー発行部135）とを備えることを特徴とする。

#### 【0061】

前記第1または第2の親機との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段（例えば、図19のステップS342, S343の処理を実行する共通秘密鍵認証部133）をさらに備えるようにすることができる。

#### 【0062】

前記第1と第2の親機の電子バリューを記憶する記憶手段（例えば、図15のバリュー記憶部140）をさらに備え、前記電子バリュー振込み手段は、前記記憶手段に記憶された電子バリューを書き換えることにより、前記第2の親機から前記第1の親機に対して、前記電子バリューを振り込むようにすることができる。

。

#### 【0063】

前記電子バリュー振込み手段は、前記第2の親機から電子バリューを取得し、その電子バリューを前記第1の親機に送信することにより、前記第2の親機から前記第1の親機に対して、前記電子バリューを振り込むようにすることができる。

。

#### 【0064】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

#### 【0065】

請求項 26 の情報処理方法、および請求項 27 のプログラムにおいて、ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第 2 の親機からの要求に応じて行う電子バリュー振込みステップ（例えば、図 16 のステップ S 167）と、前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信ステップ（例えば、図 19 のステップ S 344）とを含むことを特徴とする。

#### 【0066】

図 1 は、本発明を適用した情報処理システム 1 の構成例を示すブロック図である。この情報処理システム 1 では、親機 12 とバリュー発行装置 14 間の処理を安全確実に行うために用いられた公開鍵暗号（PKI（Public Key Infrastructure））系の暗号技術を用いてセキュリティを確保する。

#### 【0067】

図 1 の例においては、2 人のユーザが、それぞれ移動端末装置 11-1 と移動端末装置 11-2 を有している。ユーザは、必ず 1 つの親機にユーザの個人情報（利用履歴、嗜好、決済関連等）を格納し、ユーザの認証情報として共通秘密鍵を取得する。この例では、ユーザと親機が共通秘密鍵として同じパスフレーズを有しており、ユーザと親機は、同じパスフレーズを有することを確認することで、ユーザを認証する。

#### 【0068】

また、この例では、移動端末装置 11-1 のユーザは親機 12-1 に、移動端末装置 11-2 のユーザは親機 12-2 に、ユーザの個人情報を格納している。

#### 【0069】

さらに、移動端末装置 11-1 は、その移動端末装置 11-1 のユーザの個人情報を格納した親機 12-1 と直接無線で通信可能な位置にあり、移動端末装置



11-2は、その移動端末装置11-2のユーザの個人情報を格納した親機12-2とは遠隔地に設置された、親機12-1と直接無線で通信できる位置にある。従って、移動端末装置11-2は、親機12-2とは無線で通信することが困難であるが、親機12-1とは直接無線で通信できる。

#### 【0070】

移動端末装置11-1と移動端末装置11-2は、ユーザとともに移動し、無線通信を用いてユーザからの指示に対応する信号を親機12-1に送信する。また、移動端末装置11-1と移動端末装置11-2は、無線通信を用いて、親機12-1からの信号を受信する。

#### 【0071】

以下、移動端末装置11-1と移動端末装置11-2のそれぞれを個々に区別する必要がない場合、適宜、まとめて、移動端末装置11と称する。

#### 【0072】

この移動端末装置11とユーザとは、依存関係がなく、ユーザが移動端末装置11を利用するときのみ、移動端末装置11は、ユーザの認証を行う。従って、移動端末装置11には、ユーザの認証情報の入力機能が備えられている。

#### 【0073】

図1の例においては、移動端末装置11-1および移動端末装置11-2のユーザは、ユーザの認証情報として、共通秘密鍵31および共通秘密鍵32を、それぞれ入力している。

#### 【0074】

親機12-1は、所定の空間に配置され、無線通信を用いて、移動端末装置11から送信された信号を受信するとともに、移動端末装置11に信号を送信する。また、親機12-1は、ユーザに提供する情報であるコンテンツ等のリソースを有するリソース機器15-1、リソース機器15-2、リソース機器16-1、およびリソース機器16-2と接続されている。さらに、親機12-1は、インターネット21を介して、認証装置13およびバリュウ発行装置14と接続されている。

#### 【0075】

ここで、親機 12-1 は、例えば、移動端末装置 11-1 のユーザのユーザ宅の、いわゆるホームサーバで構成することができる。同様に、親機 12-2 も、例えば、移動端末装置 11-2 のユーザのユーザ宅のホームサーバで構成することができる。

#### 【0076】

以下、リソース機器 15-1 とリソース機器 15-2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器 15 と称する。また、リソース機器 16-1 とリソース機器 16-2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器 16 と称する。

#### 【0077】

これにより、移動端末装置 11 は、親機 12-1 を介して、親機 12-1 に接続されたリソース機器 15、リソース機器 16、およびインターネット 21 を介して接続された機器との通信ができる。

#### 【0078】

また、親機 12-1 は、ユーザの認証情報として共通秘密鍵 33 を格納している。即ち、この共通秘密鍵 33 は、移動端末装置 11-1 のユーザに入力された共通秘密鍵 31 と等しくなっている。さらに、親機 12-1 は、バリュ発行装置 14 により送信された共通秘密鍵 34 と、自らの正当性を証明する秘密鍵 35 を記憶している。

#### 【0079】

親機 12-2 は、インターネット 21 を介して、親機 12-1、認証装置 13、およびバリュ発行装置 14 と接続されている。

#### 【0080】

また、親機 12-2 は、ユーザの認証情報として共通秘密鍵 36 を格納している。この共通秘密鍵 36 は、移動端末装置 11-2 のユーザに入力された共通秘密鍵 32 と等しくなっている。さらに、親機 12-1 は、バリュ発行装置 14 により送信された共通秘密鍵 37 と、自らの正当性を証明する秘密鍵 38 を記憶している。

#### 【0081】

以下、親機 12-1 と親機 12-2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、親機 12 と称する。

#### 【0082】

認証装置 13 は、親機 12-1 の秘密鍵 35 に対応する公開鍵 39、親機 12-2 の秘密鍵 38 に対応する公開鍵 40、およびバリュウ発行装置 14 の後述する秘密鍵 43 に対応する公開鍵 41 を記憶する。また、認証装置 13 は、自らの正当性を証明する秘密鍵 42 を記憶する。

#### 【0083】

認証装置 13 は、他の装置からの要求に応じて公開鍵を検索し、その公開鍵を他の装置に送信する。秘密鍵とそれに対応する公開鍵は、一方の鍵に基づいて生成された暗号文を他方の鍵を用いて復号できる関係にある。また、認証装置 13 は、電子証明書 (図 11) の発行および鍵の失効管理を行う。

#### 【0084】

バリュウ発行装置 14 は、親機 12-1 と親機 12-2 に対し、バリュウ (電子バリュウ) の発行および流通管理を行う。バリュウ発行装置 14 は、自らの正当性を証明する秘密鍵 43 および共通秘密鍵 44 を記憶している。バリュウ発行装置 14 は、共通秘密鍵 44 をバリュウを発行する相手である親機 12-1 と親機 12-2 に送信し、親機 12-1 に共通秘密鍵 34 として記憶させるとともに、親機 12-2 に共通秘密鍵 37 として記憶させる。即ち、共通秘密鍵 34、共通秘密鍵 37、および共通秘密鍵 44 は等しい。

#### 【0085】

ユーザは、自身の個人情報 (利用履歴、嗜好、決済関連情報等) を自身の親機にのみ格納し、共通秘密鍵を取得する。そして、この共通秘密鍵を用いて、全ての通信を行うことにより、ユーザは、匿名性を保ち、安全に通信を行うことができる。

#### 【0086】

なお、上述の例では、2 個の移動端末装置が存在するが、移動中のユーザが多数いる場合、その数だけの移動端末装置が存在するものとする。また、上述の例では、2 個の親機が存在するが、各空間には、それぞれの空間に必要な数だけの

親機が存在するものとする。

#### 【0087】

また、共通秘密鍵 31 と共通秘密鍵 32 は、移動端末装置 11 のユーザを認証するための鍵である。共通秘密鍵 34、共通秘密鍵 37、および共通秘密鍵 44 は、バリューを扱う正当な装置であることを認証するための鍵である。秘密鍵 35、秘密鍵 38、および秘密鍵 43 は、自らの正当性を証明するための鍵であり、装置間における通信中の改ざんを防止する。

#### 【0088】

以上のように構成される通信システム 1 によって、例えば、移動端末装置 11-2 のユーザがその個人情報を記憶していない親機 12-1 のリソースを利用する場合には、移動端末装置 11-2 は、親機 12-1 の利用したいリソースを指定し、個人情報を記憶している親機 12-2 に、そのリソースの利用を要求する。親機 12-2 は、移動端末装置 11-2 からリソースが要求されると、親機 12-1 に対するリソース利用に必要なバリューの支払いを、バリュー発行装置 14 に要求する。

#### 【0089】

バリュー発行装置 14 は、親機 12-2 のバリューを親機 12-1 に移動させ、親機 12-1 にバリューの振込みが行われたことを表す振込み通知を発行する。親機 12-1 は、バリュー発行装置 14 から振り込み通知を受信すると、親機 12-2 にリソースを利用する利用権を発行する。親機 12-2 は、親機 12-1 から利用権が発行されると、その利用権を移動端末装置 11-2 に送信する。移動端末装置 11-2 は、その利用権を親機 12-1 に提示し、リソースを要求する。親機 12-2 は、移動端末装置 11-2 から利用権を提示された場合、リソースの利用を許可する。

#### 【0090】

次に、図 2 は、図 1 の移動端末装置 11 の詳細構成例を示している。

#### 【0091】

図 2 の例では、移動端末装置 11-1 を説明するが、移動端末装置 11-2 も同様に構成される。

## 【0092】

移動端末装置 11-1 は、CPU (Central Processing Unit) 61、ROM (Read Only Memory) 62、RAM (Random Access Memory) 63、表示部 64、リーダライタ 65、送信部 66、アンテナ 67、受信部 68、暗号/復号部 69、および操作入力部 70 から構成される。

## 【0093】

なお、移動端末装置 11-1 のユーザは、あらかじめ取得した共通秘密鍵 31、自身の親機 12-1 が接続しているリソースの情報、および自身の親機 12-1 のネットワーク上のアドレスを格納した非接触 IC (Integrated Circuit) カード 71 を有している。

## 【0094】

このように、共通秘密鍵 31 を改ざんが困難な非接触 IC カードに安全に格納することにより、通信システムの安全性と利便性を向上させることができる。また、非接触 IC カードは、非接触のインターフェースであるので、利用時の利便性が向上し、かつ簡単な操作で処理が可能になる。

## 【0095】

この非接触 IC カードとしては、例えば、FeliCa (商標) のような対タンパ性の高い IC チップが用いられる。なお、共通秘密鍵 31 などは、非接触型ではなく接触型のデバイスに格納することも可能である。但し、便利性及びデバイスの劣化に対する耐性を考えると、接触型ではなく、非接触型を採用するのが望ましい。

## 【0096】

CPU 61 は、ROM 62 に記憶されているプログラムに従って各種の処理を実行する。RAM 63 には、CPU 61 が各種の処理を実行する上において必要なデータなどが適宜記憶される。

## 【0097】

表示部 64 は、CPU 61 からの指令により、例えば、移動端末装置 11-1 が利用できるリソースの情報を表示する。リーダライタ 65 は、ユーザが有する非接触 IC カード 71 に封じ込められた (格納された) 共通秘密鍵 31、ユーザの

個人情報記憶した親機 12-1 が接続しているリソースの情報、および個人情報記憶した親機 12-1 のネットワーク上のアドレスを読み込み、CPU 61 に共通秘密鍵 31、リソース情報、およびアドレスを供給する。ここで、また、リーダーライタ 65 は、CPU 61 からの指令により、必要に応じて非接触 IC カード 71 にデータを書き込む。

#### 【0098】

送信部 66 は、CPU 61 からの指令により、親機 12-1 に送信する信号をアンテナ 67 に供給する。アンテナ 67 は、送信部 66 から供給された信号を、無線通信を用いて親機 12-1 に送信する。さらに、アンテナ 67 は、親機 12-1 から送信された信号を受信し、その信号を受信部 68 に供給する。受信部 68 は、アンテナ 67 から供給された信号を、CPU 61 に供給する。

#### 【0099】

暗号/復号部 69 は、非接触 IC カード 71 から読み込まれた共通秘密鍵 31 を暗号化したり、受信部 68 で受信した暗号化された共通秘密鍵を復号し、その復号した共通秘密鍵をさらに暗号化する。操作入力部 70 は、ユーザにより操作され、その操作に対応する信号が CPU 61 に供給される。

#### 【0100】

図 3 は、図 2 の移動端末装置 11 がリソースを取得する処理を説明するフローチャートである。なお、ユーザは、予め個人情報を自身の親機に格納しており、共通秘密鍵 31 (32)、その親機に接続されているリソースの情報、およびその親機のネットワーク上のアドレスは非接触 IC カード 71 に記憶されているものとする。図 3 の処理は、例えば、ユーザが操作入力部 70 を操作して親機 12-1 に接続されているリソースの取得を要求したときに開始される。

#### 【0101】

ステップ S1 において、CPU 61 は、移動端末装置 11 を使用するユーザの個人情報が格納されている自身の親機（以下、適宜、本親機と称する）と無線通信が可能であるかどうかを判定する。例えば、移動端末装置 11 は、無線通信が可能な機器を検索し、検索された機器の中に本親機が含まれているかどうかを判定する。

## 【0102】

ステップS1で、CPU61は、本親機と無線通信が可能であると判定した場合、ステップS2に進み、CPU61は、本親機（例えば、移動端末装置11-1の場合、親機12-1）との間で共通秘密鍵認証処理を行ない、ステップS3に進む。この共通秘密鍵認証処理の詳細は、図4で後述する。

## 【0103】

ステップS3では、CPU61は、ユーザが操作入力部70を操作することにより指定したリソースを要求する信号を、送信部66を制御して、アンテナ67から本親機である、例えば、親機12-1に送信する。即ち、ユーザは、非接触ICカード71に記憶され、リーダライタ65から読み込まれたリソース情報を表示部64に表示させ、そのリソース情報を見て、取得したいリソースを指定する。これにより、そのリソースを要求する信号がアンテナ67から送信される。なお、以下の説明では、CPU61が送信部66を制御して、信号を送信することを、単に、CPU61が信号を送信するという。

## 【0104】

ステップS3の処理後は、ステップS4に進み、アンテナ67は、ステップS3のリソース要求信号に対応して親機12-1から送信されたリソース（を使用するのに必要な情報）を受信し、受信部68を介してCPU61に供給する。そして、CPU61は、そのリソースをRAM63に保持する。なお、以下の説明では、アンテナ67が信号を受信し、受信部68を介して、CPU61にその信号を供給することを、単に、CPU61が信号を受信するという。

## 【0105】

一方、ステップS1で、CPU61は、本親機と無線通信が可能ではないと判定した場合（例えば、移動端末装置11-2が、親機12-2と通信できない場合）、ステップS5に進み、リソース情報取得処理を行ない、ステップS6に進む。即ち、例えば、移動端末装置11-2については、現在、その移動端末装置11-2と通信できる親機12-1が本親機ではないので、移動端末装置11-2は、親機12-1が接続しているリソースの情報を非接触ICカード71に記憶していない。従って、移動端末装置11-2は、親機12-1が接続しているリ

ソースの情報を取得する必要があるため、ステップS5において、リソース情報取得処理が行なわれる。このリソース情報取得処理の詳細は、図5で後述する。

#### 【0106】

ステップS6において、CPU61は、本親機（親機12-2）との間で共通秘密鍵認証処理を行い、ステップS7に進む。なお、いまの場合、移動端末装置11-2は、本親機である親機12-2と直接無線通信することはできないため、ステップS6の共通秘密鍵認証処理は、後述するように、移動端末装置11-2と親機12-2との間で、親機12-1およびインターネット21を介した通信を行うことにより実行される。この共通秘密鍵認証処理の詳細は、図4で後述する。

#### 【0107】

ステップS7では、CPU61は、非接触ICカード71から、親機12-2のアドレスを読み出す。そして、ユーザが操作入力部70を操作することにより指定したリソースを要求する信号（リソース利用権発行要求）を親機12-2のアドレスとともに、親機12-1に送信し、インターネット21経由で親機12-2に送信する。即ち、ユーザは、ステップS5で取得した親機12-1が接続しているリソースのリソース情報を表示部64に表示させ、そのリソース情報を見て、取得したいリソースを指定する。これにより、そのリソースを利用する権利を要求する信号として、リソース利用権発行要求が、移動端末装置11-2から、親機12-1およびインターネット21を介して、本親機である親機12-2に送信される。

#### 【0108】

ここで、移動端末装置11-2は、上述のように、親機12-2のアドレスを親機12-1に知らせる。これにより、移動端末装置11-2は、無線通信可能な親機12-1とインターネット21を介して、本親機である親機12-2と通信が可能になる。

#### 【0109】

ステップS7の処理後は、ステップS8に進み、CPU61は、親機12-1か



ら、リソースを取得する権利を記載した権利文のデータであるリソース利用権を受信したか否かを判定する。ステップS 8で、CPU 6 1は、親機 1 2-1 から権利文を受信したと判定した場合、移動端末装置 1 1-2 は、親機 1 2-1 に接続しているリソースを利用する権利があるので、ステップS 9に進み、親機 1 2-1 に、受信した権利文とリソース要求信号を送信する。ステップS 9の処理後は、ステップS 10に進み、CPU 6 1は、リソース要求信号に対応して、親機 1 2-1 から送信されたリソース（を利用するのに必要な情報）を受信し、そのリソースをRAM 6 3に保持して、処理を終了する。

#### 【0110】

この場合、移動端末装置 1 1-2 は、本親機でない親機 1 2-1 のリソースを使用することができる。

#### 【0111】

一方、ステップS 8で、CPU 6 1は、親機 1 2-1 から権利文を受信していないと判定した場合、ステップS 11に進み、親機 1 2-2 から、親機 1 2-1 を介して、リソースを取得する権利を記載した権利文を発行できないことを示すエラー通知を受信したか否かを判定する。ステップS 11で、CPU 6 1は、親機 1 2-1 からエラー通知を受信していないと判定した場合、ステップS 8に戻り、上述した処理を繰り返す。

#### 【0112】

また、ステップS 11において、CPU 6 1は、親機 1 2-2 からエラー通知を受信したと判定した場合、移動端末装置 1 1-2 は、親機 1 2-1 に接続しているリソースを取得する権利がないので、処理を終了する。

#### 【0113】

図4は、図3のステップS 2とステップS 6の共通秘密鍵認証処理を説明するフローチャートである。この処理は、移動端末装置 1 1とそのユーザの本親機との間で行われる。

#### 【0114】

図4の例では、移動端末装置 1 1-1における共通秘密鍵認証処理を説明するが、移動端末装置 1 1-2における場合も同様の処理が行われる。但し、移動端

末装置 11-2 の場合は、本親機である親機 12-2 と無線通信が可能ではないので、無線通信可能な親機 12-1 にその本親機である親機 12-2 のアドレスを通知し、親機 12-1 を介して、インターネット 21 経由で本親機である親機 12-2 と通信する。

#### 【0115】

ステップ S21 において、CPU 61 は、リーダライタ 65 を制御して、非接触 IC カード 71 から、ユーザの認証情報である共通秘密鍵 31 を読み込み、RAM 63 に保持する。ステップ S21 の処理後は、ステップ S22 に進み、CPU 61 は、共通秘密鍵 31 を暗号化し、ステップ S23 に進む。即ち、移動端末装置 11-1 は、認証装置 13 から親機 12-1 (本親機) の秘密鍵 35 に対応する公開鍵 39 を取得し、RAM 63 に保持する。CPU 61 は、RAM 63 に保持した公開鍵 39 を、共通秘密鍵 31 とともに暗号/復号部 69 に供給する。暗号/復号部 69 は、その公開鍵 39 を用いて、共通秘密鍵 31 を暗号化する。

#### 【0116】

ステップ S23 では、CPU 61 は、ステップ S22 で暗号化した共通秘密鍵 31 を、本親機である親機 12-1 に送信し、ステップ S24 に進む。ステップ S24 において、CPU 61 は、親機 12-1 (本親機) から、後述する図 8 のステップ S64 で送信されてくる秘密鍵 35 で暗号化された共通秘密鍵 33 を受信したかどうかを判定し、暗号化された共通秘密鍵 33 を受信していないと判定した場合、受信されるまで待機する。

#### 【0117】

ステップ S24 において、CPU 61 は、親機 12-1 から暗号化された共通秘密鍵 33 を受信したと判定した場合、ステップ S25 に進み、暗号/復号部 69 を制御し、その暗号化された共通秘密鍵 33 を、ステップ S22 の処理で RAM 63 に保持した、秘密鍵 35 と対の公開鍵 39 を用いて復号する。このとき、秘密鍵 35 とそれに対応する公開鍵 39 は、一方の鍵に基づいて生成された暗号文 (パスフレーズ) を他方の鍵を用いて復号できる関係にあるので、秘密鍵 35 に基づいて暗号化された共通秘密鍵 33 (パスフレーズ) が、親機 12-1 から送信され、移動端末装置 11-1 で受信されるまでの間に改ざんされなかった場合、

その暗号化された共通秘密鍵 33 は、公開鍵 39 に基づいて復号されると、共通秘密鍵 33 となる。

#### 【0118】

ステップ S25 の処理後は、ステップ S26 に進み、CPU61 は、暗号/復号部 69 を制御して、復号した共通秘密鍵 33 を、ステップ S22 の処理で RAM63 に保持した公開鍵 39 を用いて暗号化し、その暗号化した共通秘密鍵を親機 12-1 (本親機) に送信し、ステップ S27 に進む。ステップ S27 において、CPU61 は、親機 12-1 (本親機) から、後述する図 8 のステップ S68 の処理で秘密鍵 35 を用いて暗号化された共通秘密鍵 (親機 12-1 が、ステップ S23 で親機 12-1 に送信された暗号化した共通秘密鍵 31 を秘密鍵 35 を用いて復号し、さらに暗号化した共通秘密鍵) 31 を受信したかどうかを判定する。

#### 【0119】

ステップ S27 で、CPU61 は、親機 12-1 から暗号化された共通秘密鍵 31 を受信したと判定した場合、ステップ S28 に進み、暗号/復号部 69 を制御して、その暗号化された共通秘密鍵 31 を、秘密鍵 35 と対の RAM63 に保持した公開鍵 39 を用いて復号する。ステップ S28 の処理後は、ステップ S29 に進み、ステップ S28 で復号された共通秘密鍵が、ステップ S21 で RAM63 に保持された共通秘密鍵 31 と等しいかどうかを判定する。

#### 【0120】

ステップ S29 において、CPU61 は、復号された共通秘密鍵 31 が、RAM63 に保持された共通秘密鍵 31 と等しいと判定した場合、図 3 のステップ S3 または図 3 のステップ S7 にリターンする。即ち、この場合、ステップ S23 で公開鍵 39 を用いて暗号化された共通秘密鍵 31 が、親機 12-1 により秘密鍵 35 を用いて正常に復号され、共通秘密鍵 31 が得られている。そして、その共通秘密鍵 31 が、親機 12-1 において秘密鍵 35 を用いて暗号化され、その暗号化された共通秘密鍵 31 が、移動端末装置 11-1 において、公開鍵 39 を用いて正常に復号され、共通秘密鍵 31 が得られている。

#### 【0121】

従って、秘密鍵 35 とそれに対応する公開鍵 39 は、一方の鍵に基づいて暗号

化された共通秘密鍵 31 を他方の鍵を用いて復号できる関係にあるので、移動端末装置 11-1 は、移動端末装置 11-1 と親機 12-1 が通信する間で改ざんがなかったことを認識できる。

#### 【0122】

一方、ステップ S29 において、CPU 61 は、ステップ S28 で復号された共通秘密鍵が、RAM 63 に保持された共通秘密鍵 31 と等しくないと判定した場合、秘密鍵 35 とそれに対応する公開鍵 39 は、一方の鍵に基づいて生成された共通秘密鍵 31 を他方の鍵を用いて復号できる関係にないので、移動端末装置 11-1 と親機 12-1 が通信する間で改ざんがあった、あるいは、親機 12-1 が正当な装置でないと認識し、処理を終了する。

#### 【0123】

このように、移動端末装置 11-1 は、移動端末装置 11-1 と親機 12-1 が通信する間で改ざんがなかったと認識できたときのみ、図 3 のステップ S3 または図 3 のステップ S7 に進み、親機 12-1 にリソースを要求する信号を送信するので、移動端末装置 11-1 と親機 12-1 の両者間での通信中のデータ秘匿が可能となる。

#### 【0124】

一方、ステップ S27 において、CPU 61 は、親機 12-1 から暗号化された共通秘密鍵 31 を受信していないと判定した場合、ステップ S30 に進み、後述する図 8 のステップ S71 で親機 12-1 が送信した、親機 12-1 と移動端末装置 11-1 の関係が正当ではないことを示すエラー通知を受信したか否かを判定する。ステップ S30 において、CPU 61 は、親機 12-1 からエラー通知を受信していないと判定した場合、ステップ S27 に戻り、上述した処理を繰り返す。

#### 【0125】

一方、ステップ S30 において、CPU 61 は、親機 12-1 からエラー通知を受信したと判定した場合、親機 12-1 と移動端末装置 11-1 の関係は正当ではないので、処理を終了する。

#### 【0126】

図5は、図3のステップS5の処理を説明するフローチャートである。

【0127】

ステップS41において、例えば、移動端末装置11-2のCPU61は、直接無線通信することができる本親機でない親機12-1にブロードキャストを要求する。即ち、移動端末装置11-2は、ブロードキャスト要求（デバイス探索）等によって、親機12-1が管理する機器（例えば、リソース機器15-1等）や電子権利などのリソース情報を取得する。

【0128】

ステップS41の処理後は、ステップS42に進み、CPU61は、親機12-1から、ブロードキャスト要求を許可された（後述する図12のステップS121で送信されたブロードキャスト要求許可の通知を受信した）かどうかを判定する。ステップS42において、CPU61は、親機12-1からブロードキャスト要求が許可されたと判定した場合、ステップS43に進み、親機12-1にリソース情報を要求する。

【0129】

ステップS43の処理後は、ステップS44に進み、CPU61は、リソース情報要求に対応して、親機12-1から送信されたリソース情報を受信し、そのリソース情報をRAM63に保持する。

【0130】

一方、ステップS42において、CPU61は、親機12-1から、ブロードキャスト要求を許可されていないと判定した場合、ステップS45に進み、ブロードキャスト要求に対応して親機12-1から送信されたブロードキャスト要求の不許可を示すエラー通知が、受信されたかどうかを判定する。ステップS45において、CPU61は、エラー通知が受信されていないと判定した場合、ステップS42に戻り、上述した処理を繰り返す。

【0131】

また、ステップS45において、CPU61は、エラー通知が受信されたと判定した場合、親機12-1にブロードキャスト要求が許可されず、親機12-1からリソース情報を得ることができないので、処理を終了する。

## 【0132】

図6は、図1の親機12の詳細構成例を示している。

## 【0133】

図6の例では、親機12-1を説明するが、親機12-2も同様に構成される。

## 【0134】

親機12-1は、CPU91、ROM92、RAM93、アンテナ94、受信部95、送信部96、入出力部97、データバス98、リソース制御部99、および通信部100から構成されている。

## 【0135】

CPU91は、ROM92に記憶されているプログラムに従って各種の処理を実行する。例えば、CPU91は、受信部95から供給された受信データの供給先を判定し、入出力部97を制御して、その供給先に、受信データを供給する。RAM93には、CPU91が各種の処理を実行する上において必要なデータなどが適宜記憶される。

## 【0136】

アンテナ94は、移動端末装置11から送信された信号を受信し、その信号を受信部95に供給する。また、アンテナ94は、送信部96から供給された信号を移動端末装置11に送信する。

## 【0137】

受信部95は、アンテナ94から供給された信号をCPU91に供給する。送信部96は、CPU91からの指令に基づいて、移動端末装置11に送信する信号をアンテナ94に供給する。

## 【0138】

入出力部97は、データバス98を介してリソース制御部99と通信部100に接続されるとともに、リソース機器16-1とリソース機器16-2に接続されている。リソース制御部99は、リソース機器15-1とリソース機器15-2にそれぞれ接続されている。

## 【0139】

通信部 100 は、CPU 91 からの指令に基づき、インターネット 21 を介して、親機 12-2、認証装置 13、およびバリュー発行装置 14 に信号を送信するとともに、親機 12-2、認証装置 13、およびバリュー発行装置 14 から信号を受信する。

#### 【0140】

図 7 は、図 6 のリソース制御部 99 の詳細構成例を示している。

#### 【0141】

リソース制御部 99 は、CPU 111、ROM 112、RAM 113、入出力部 114、リーダライタ 115、表示部 116、および暗号/復号部 117 から構成される。

#### 【0142】

CPU 111 は、ROM 112 に記憶されているプログラムに従って各種の処理を実行する。RAM 113 は、ユーザの個人情報を格納しており、CPU 111 は、個人情報を管理している。また、RAM 113 には、CPU 111 が各種の処理を実行する上において必要なデータなどが適宜記憶される。

#### 【0143】

CPU 111 は、入出力部 114 を介して、リソース機器 15-1 とリソース機器 15-2 に接続されており、リソース機器 15-1 とリソース機器 15-2 から供給されたリソースを、データバス 98 および入出力部 97 を介して、CPU 91 に供給する。リーダライタ 115 は、親機 12-1 に備えられた非接触 IC カード 121 から、データを読み込んだり、データを書き込む。

#### 【0144】

非接触 IC カード 121 には、個人認証用の情報の格納領域と電子バリューのための認証用の情報の格納領域が設けられている。個人認証用の情報の格納領域には、移動端末装置 11-1 の共通秘密鍵 31 と同一の共通秘密鍵 33 と自らの正当性を証明するための秘密鍵 35 が格納されている。電子バリューのための認証用の情報の格納領域には、バリュー発行装置 14 により発行された共通秘密鍵 34 等が格納されている。なお、電子バリューのための認証用の情報の格納領域は、認証用と電子バリュー用の領域に分けることができる。認証用の領域には、

秘密鍵 34 が格納され、電子バリュウの領域には、電子バリュウ（例えば、権利文）が格納される。

#### 【0145】

このように、共通秘密鍵 33、共通秘密鍵 34、および秘密鍵 35 を改ざんが困難な非接触 IC カード 121 に安全に格納することにより、通信システムの安全性と利便性を向上させることができる。

#### 【0146】

表示部 116 は、CPU 111 の指令により、例えば、リソース情報を表示する。暗号/復号部 117 は、鍵、その他の情報を暗号化または復号する。

#### 【0147】

なお、親機 12-1 は、物理的に 1 つの筐体で構成する必要はなく、データバスを経由して複数の機器が協調して機能を実現するように構成してもよい。

#### 【0148】

図 8 は、図 7 の親機 12 のリソース制御部 99 がリソースを制御する処理を説明するフローチャートである。この処理は、例えば、移動端末装置 11 から信号を受信したとき開始される。

#### 【0149】

以下の説明では、親機 12-1 がリソースを制御する処理を説明するが、親機 12-2 における場合も同様の処理が行われる。

#### 【0150】

ステップ S61 では、CPU 111 は、リーダライタ 115 を制御し、非接触 IC カード 121 から共通秘密鍵 33 を読み込み、その共通秘密鍵 33 を RAM 113 に保持する。ステップ S61 の処理後は、ステップ S62 に進み、CPU 111 は、図 4 のステップ S23 で移動端末装置 11-1 から送信された暗号化した共通秘密鍵 31 が受信されたかどうかを判定する。

#### 【0151】

即ち、CPU 91 は、アンテナ 94 により受信され、受信部 95 を介して供給された信号が、親機 12-1 に対するものである場合、入出力部 97 を制御し、データバス 98 を介して、その信号をリソース制御部 99 の CPU 111 に供給し、C



PU111は、その信号が暗号化された共通秘密鍵31であるかどうかを判定する。なお、以下の説明では、このようにCPU91がアンテナ94により受信された信号をリソース制御部99のCPU111に供給することを、単に、CPU111が信号を受信するという。

#### 【0152】

ステップS62において、CPU111は、移動端末装置11-1から暗号化された共通秘密鍵31が受信されたと判定した場合、ステップS63に進み、非接触ICカード121から秘密鍵35を読み込み、その暗号化された共通秘密鍵31と秘密鍵35をRAM113に保持する。そして、CPU111は、暗号/復号部117を制御し、ステップS61でRAM113に保持した共通秘密鍵33を、秘密鍵35を用いて暗号化する。

#### 【0153】

ステップS63の処理後は、ステップS64に進み、CPU111は、ステップS62で暗号化された共通秘密鍵33を、移動端末装置11-1に送信し、ステップS64からステップS65に進む。ステップS65では、CPU111は、図4のステップS26で移動端末装置11-1から送信された暗号化された共通秘密鍵が受信されたかどうかを判定し、移動端末装置11-1から暗号化された共通秘密鍵が受信されるまで待機する。

#### 【0154】

ステップS65において、CPU111は、移動端末装置11-1から暗号化された共通秘密鍵が供給されたと判定した場合、ステップS66に進み、その暗号化された共通秘密鍵を復号し、ステップS67に進む。即ち、CPU111は、暗号/復号部117を制御し、ステップS63でRAM113に保持した、公開鍵39と対の秘密鍵35を用いて、暗号化された共通秘密鍵を復号する。

#### 【0155】

ステップS67では、CPU111は、その復号された共通秘密鍵が、RAM113に保持された共通秘密鍵33と等しいかどうかを判定する。ステップS67において、CPU111は、その復号された共通秘密鍵がRAM113に保持された共通秘密鍵33と等しいと判定した場合、ステップS68に進む。

## 【0156】

即ち、この場合、ステップS63で秘密鍵35を用いて暗号化された共通秘密鍵33が、移動端末装置11-1において、公開鍵39を用いて正常に復号され、共通秘密鍵33が得られている。そして、その秘密鍵33が移動端末装置11-1において、公開鍵39を用いて暗号化され、その暗号化された共通秘密鍵31が、親機12-1において、秘密鍵35を用いて正常に復号され、共通秘密鍵33が得られている。

## 【0157】

従って、秘密鍵35とそれに対応する公開鍵39は、一方の鍵に基づいて暗号化された共通秘密鍵33を他方の鍵を用いて復号できる関係にあるので、親機12-1は、移動端末装置11-1と親機12-1が通信する間で改ざんがなかったことが認識できる。

## 【0158】

その後、ステップS68において、CPU111は、ステップS62で移動端末装置11-1から受信し、RAM113に保持した暗号化された共通秘密鍵31を、RAM113に保持した公開鍵39と対の秘密鍵35を用いて復号する。

## 【0159】

ステップS68の処理後は、ステップS69に進み、CPU111は、ステップS68で復号した共通秘密鍵が、RAM113に保持した共通秘密鍵33と等しいかどうかを判定する。ステップS69において、CPU111は、その復号した共通秘密鍵がRAM113に保持した共通秘密鍵33と等しいと判定した場合、ステップS70に進む。

## 【0160】

即ち、この場合、図4のステップS22で移動端末装置11-1により公開鍵39を用いて暗号化された、秘密鍵33と同一の共通秘密鍵31が、ステップS68で親機12-1により秘密鍵35を用いて正常に復号され、共通秘密鍵31が得られている。そして、移動端末装置11-1が有する共通秘密鍵31と親機12-1が有する共通秘密鍵33が同一であることが検証、つまり、移動端末装置11-1のユーザが、親機12-1のユーザであることが検証されている。

## 【0161】

従って、秘密鍵 35 とそれに対応する公開鍵 39 は、一方の鍵に基づいて暗号化された共通秘密鍵 31 を他方の鍵を用いて復号できる関係にあるので、親機 12-1 は、移動端末装置 11-1 と親機 12-1 が通信する間で改ざんがなかったことが認識できる。また、移動端末装置 11-1 が有する共通秘密鍵 31 と親機 12-1 が有する共通秘密鍵 33 が等しくなっているため、親機 12-1 は、移動端末装置 11-1 のユーザが個人情報を格納したユーザであることを認識する。

## 【0162】

その後、ステップ S70 において、暗号/復号部 69 を制御して、その復号した共通秘密鍵を、RAM 113 に保持した秘密鍵 35 を用いて暗号化し、移動端末装置 11-1 に送信する。

## 【0163】

一方、ステップ S67 において、CPU 111 は、ステップ S66 で復号された共通秘密鍵が RAM 113 に保持する共通秘密鍵 33 と等しくないと判定した場合、またはステップ S69 で、ステップ S68 で復号された共通秘密鍵が RAM 113 に保持する共通秘密鍵 33 と等しくないと判定した場合、移動端末装置 11-1 と親機 12-1 が通信する間で改ざんがあったか、または親機 12-1 が移動端末装置 11-1 の本親機ではないので、ステップ S71 に進み、移動端末装置 11-1 と親機 12-1 の関係が正当ではないことを示すエラー通知を送信し、処理を終了する。

## 【0164】

このように、親機 12-1 は、移動端末装置 11-1 と親機 12-1 が通信する間で改ざんがなく、かつ移動端末装置 11-1 の本親機であると認識できたときのみ、復号した共通秘密鍵 31 を暗号化して移動端末装置 11-1 に送信する。

## 【0165】

この後、移動端末装置 11-1 は、移動端末装置 11-1 と親機 12-1 が通信する間で改ざんがなかったと認識できたときのみリソースを要求する信号を親

機 12-1 に送信するので、移動端末装置 11-1 は、移動端末装置 11-1 と親機 12-1 が通信する間で改ざんがなかったと移動端末装置 11-1 と親機 12-1 の両方で認識（双方向認証）され、かつ親機 12-1 が移動端末装置 11-1 の本親機である場合のみ、リソースを要求し、利用することができる。

#### 【0166】

これにより、移動端末装置 11-1 と親機 12-1 の両者間での通信中のデータ秘匿が可能となる。

#### 【0167】

ステップ S62 において、CPU 111 は、移動端末装置 11-1 からリソース要求信号が供給されたと判定した場合、ステップ S73 に進み、リソース送信処理を行い、その後、処理を終了する。リソース送信処理の詳細は、図 9 と図 10 で後述する。

#### 【0168】

一方、ステップ S72 において、CPU 111 は、リソース要求信号が供給されていないと判定した場合、ステップ S62 に戻り、上述した処理を繰り返す。

#### 【0169】

図 9 は、移動端末装置 11-1 および 11-2 と直接無線通信が可能な親機 12-1 が図 8 のステップ S73 の処理で行うリソース送信処理を説明するフローチャートである。

#### 【0170】

ステップ S81 において、親機 12-1 の CPU 111 は、図 8 のステップ S72 で受信したリソース要求信号が自身が本親機となる移動端末装置（移動端末装置 11-1）からのリソース要求信号であるかどうかを判定する。ステップ S81 において、親機 12-1 の CPU 111 は、受信したリソース要求信号が自身が本親機となる移動端末装置 11-1 からのリソース要求信号であると判定した場合、ステップ S82 をスキップしてステップ S83 に進む。

#### 【0171】

ステップ S83 では、親機 12-1 の CPU 111 は、入出力部 114 を制御し、移動端末装置 11-1 からのリソース要求信号に基づいて、移動端末装置 11

ー 1 から要求されているリソースを有するリソース機器 15 からリソースを取得し、ステップ S 84 に進む。ステップ S 84 では、親機 12-1 の CPU 111 は、そのリソースを、移動端末装置 11-1 に送信してリターンする。

#### 【0172】

即ち、親機 12-1 は、個人情報情報を格納しているユーザが使用する移動端末装置 11-1 から、親機 12-1 の接続するリソース機器 15 の有するリソースを要求された場合、無条件に利用を許可する。

#### 【0173】

一方、ステップ S 81 において、親機 12-1 の CPU 111 は、図 8 のステップ S 72 で受信したリソース要求信号が、自身が本親機とならない移動端末装置からのリソース要求信号である（移動端末装置 11-2 からのリソース要求信号である）と判定した場合、ステップ S 82 に進み、権利文の提示がある（リソース要求信号とともに権利文が送信されてきた）かどうかを判定する。ステップ S 82 において、親機 12-1 の CPU 111 は、権利文の提示がなかったと判定した場合、移動端末装置 11-2 はリソースを利用する権利がないので、処理を終了する。

#### 【0174】

ステップ S 82 において、親機 12-1 の CPU 111 は、権利文の提示があったと判定した場合、ステップ S 83 に進み、入出力部 114 を制御し、移動端末装置 11-2 からのリソース要求信号に基づいて、移動端末装置 11-2 から要求されているリソースを有するリソース機器 15 からリソースを取得し、ステップ S 84 に進む。ステップ S 84 では、親機 12-1 の CPU 111 は、そのリソースを、移動端末装置 11-2 に送信する。

#### 【0175】

即ち、親機 12-1 は、個人情報情報を格納していないユーザが使用する移動端末装置 11-2 から、親機 12-1 に接続しているリソース機器 15 の有するリソースを要求された場合、移動端末装置 11-2 がリソースを利用する権利文を取得している場合のみ、リソース利用を許可する。逆に言えば、移動端末装置 11-2 のユーザは、本親機 12-1 のリソースを、そのリソースを利用する権利文

を、親機 12-1 に提示したときのみ利用することができる。

#### 【0176】

なお、親機 12-1 は、親機 12-2 が移動端末装置 11-2 のユーザを認証するときのやりとり時に、移動端末装置 11-2 は、そのユーザの個人情報を、その本親機である親機 12-2 から取得する。ここで、個人情報には、そのユーザがリソースを利用したときの操作履歴などが含まれる。即ち、移動端末装置 11-2 の本親機である親機 12-2 は、例えば、そのユーザが自身の有するリソースを利用したときに、その利用時の操作履歴などを個人情報として登録する個人情報管理機能を有する。移動端末装置 11-2 は、親機 12-1 のリソースを利用するときに、ユーザの個人情報に応じて、移動端末装置 11-2 のユーザの嗜好に合わせた操作性（ユーザ I/F）を提供する。

#### 【0177】

図 10 は、移動端末装置 11-2 がその本親機である親機 12-2 と直接無線通信できない場合に、その親機 12-2 が図 8 のステップ S71 の処理で行うリソース送信処理を説明するフローチャートである。なお、親機 12-2 は、認証装置 13 から発行された電子証明書（図 11 で後述する）を既に受信し、RAM 13 に保持しているものとする。

#### 【0178】

ステップ S100 において、親機 12-2 の CPU 111 は、暗号化した利用権発行要求文と、RAM 113 に保持している電子証明書を作成し、その利用権発行要求文と電子証明書を、移動端末装置 11-1 がリソースを利用しようとする本親機でない親機 12-1 に送信する。即ち、親機 12-2 の CPU 111 は、直接無線通信することができない移動端末装置 11-2 から送信されたリソース要求信号に基づいて、リソース情報の識別子と利用方法を明記した利用権発行要求文を作成する。

#### 【0179】

また、親機 12-2 の CPU 111 は、リーダライタ 115 を制御し、非接触 IC カード 121 から読み込んだ秘密鍵 38 を RAM 113 に保持する。CPU 111 は、暗号/復号部 117 を制御し、RAM 113 に保持した秘密鍵 38 を用いて、電子

署名を暗号化し、利用権発行要求文を付加する。そして、CPU 111は、その利用権発行要求文を電子証明書とともに、移動端末装置 11-2 がリソースを利用しようとしている親機 12-1 に送信する。

#### 【0180】

なお、利用権発行要求文とは、ここでは、移動端末装置 11-2 が、その本親機でない親機 12-1 のリソースの利用をするための利用権の発行を、親機 12-1 に要求するメッセージである。

#### 【0181】

また、移動端末装置 11-2 が本親機である親機 12-2 に送信するリソース要求信号には、その移動端末装置 11-2 がリソースを利用しようとする本親機でない親機 12-2 へアクセスするためのアクセス情報が含まれている。そして、親機 12-2 は、このアクセス情報に基づいて、利用権発行要求文を親機 12-1 に送信する。

#### 【0182】

ステップ S100 の処理後は、ステップ S101 に進み、親機 12-2 の CPU 111 は、後述する図 13 のステップ S147 で、利用権はおつ光要求文を受信した親機 12-1 が親機 12-2 に対して送信するリソースの利用を許可するための対価（バリュー）と対価の送信先口座情報を記載したリソース利用条件文と電子証明書を受信したかどうかを判定する。ステップ S101 において、親機 12-2 の CPU 111 は、リソース利用条件文と電子証明書を受信したと判定した場合、暗号/復号部 117 を制御し、電子証明書に含まれる、親機 12-1 の秘密鍵 35 に対応する公開鍵 39 を用いて、リソース利用条件文に含まれる電子署名を復号し、ステップ S101 からステップ S102 に進む。

#### 【0183】

ステップ S102 において、親機 12-2 の CPU 111 は、リソース利用条件文が正当であるかどうかを判定する。即ち、CPU 111 は、リソース利用条件文に含まれる電子署名が正常に復号されたかどうかを判定する。ステップ S102 において、CPU 111 は、リソース利用条件文が正当ではないと判定した場合、親機 12-1 の秘密鍵 35 で暗号化された電子署名が、それと対の公開鍵 39 で

復号できていないので、親機 12-1 と親機 12-2 が通信する間で改ざんが行われたと判定し、処理を終了する。

#### 【0184】

また、ステップ S102 において、親機 12-2 の CPU111 は、リソース利用条件文が正当であると判定した場合、秘密鍵 35 で暗号化された電子署名が、公開鍵 39 で復号できるので、親機 12-1 と親機 12-2 が通信する間で改ざんが行われず、親機 12-1 と親機 12-2 が正当な関係であると認識し、ステップ S102 からステップ S103 に進む。

#### 【0185】

このように、電子署名を用いてリソース利用条件文が正当であるかどうかを判定することにより、通信システム 1 の安全性をさらに高めることができる。

#### 【0186】

ステップ S103 において、親機 12-2 の CPU111 は、リソース利用条件文に基づいて、親機 12-2 から親機 12-1 にバリューを移動する（対価を支払う）ためのバリュー移動要求をバリュー発行装置 14 に送信する。

#### 【0187】

ステップ S103 の処理後は、ステップ S104 に進み、親機 12-2 の CPU111 は、バリュー発行装置 14 から、後述する図 16 のステップ S162 で送信される暗号化された共通秘密鍵 44 を受信したかどうかを判定する。ステップ S104 において、CPU111 は、バリュー発行装置 14 から暗号化された共通秘密鍵 44 を受信していないと判定した場合、バリュー発行装置 14 から暗号化された共通秘密鍵 44 が受信されるまで待機する。

#### 【0188】

ステップ S104 において、親機 12-2 の CPU111 は、バリュー発行装置 14 から暗号化された共通秘密鍵 44 を受信したと判定した場合、ステップ S105 に進み、親機 12-2 の CPU111 は、バリュー発行装置 14 の有する秘密鍵 43 に対応する公開鍵 41 を、認証装置 13 から取得し、RAM113 に保持する。そして、親機 12-2 の CPU111 は、暗号/復号部 117 を制御し、RAM113 に保持した公開鍵 41 を用いて、暗号化された共通秘密鍵 44 を復号し、復



号した共通秘密鍵44をRAM113に保持する。

#### 【0189】

ステップS105の処理後は、ステップS106に進み、親機12-2のCPU111は、リーダライタ115を制御して、共通秘密鍵37を読み込み、RAM113に保持し、ステップS107に進む。ステップS107では、親機12-2のCPU111は、RAM113から復号した共通秘密鍵44と共通秘密鍵37を読み出し、両者が等しいかどうかを判定する。

#### 【0190】

ステップS107において、親機12-2のCPU111は、復号した共通秘密鍵44と共通秘密鍵37が等しいと判定した場合、即ち、後述する図16のステップS161でバリュウ発行装置14により秘密鍵43を用いて暗号化された共通秘密鍵44が、ステップS106で親機12-2により公開鍵41を用いて正常に復号され、共通秘密鍵37と等しい共通秘密鍵44が得られている場合、親機12-2のCPU111は、バリュウ発行装置14と親機12-2が通信する間で改ざんがなかったことが認識し、ステップS107からステップS108に進む。

#### 【0191】

従って、CPU111は、S108では、親機12-2のCPU111は、暗号/復号部117を制御し、RAM113に保持した公開鍵41を用いて、RAM113に保持した共通秘密鍵37を暗号化する。ステップS109の処理後は、ステップS110に進み、親機12-2のCPU111は、その暗号化した共通秘密鍵37を、バリュウ発行装置14に送信し、リターンする。

#### 【0192】

一方、ステップS107において、親機12-2のCPU111は、ステップS106で復号した共通秘密鍵と共通秘密鍵34が等しくないと判定した場合、バリュウ発行装置14と親機12-2が通信する間で改ざんがあったと認識し、ステップS110に進み、バリュウ発行装置14に、バリュウ発行装置14と親機12-2の関係は正当ではないことを示すエラーを通知してリターンする。

#### 【0193】

また、ステップS101において、親機12-2のCPU111は、移動端末装置12-2がリソースを利用しようとする親機12-1からのリソース利用条件文を受信していないと判定した場合、ステップS111に進み、親機12-1から、後述する図13のステップS148で送信されたるリソース利用条件文を発行できないことを示すエラー通知を受信したかどうかを判定する。ステップS110において、親機12-2のCPU111は、親機12-1からエラー通知を受信していないと判定した場合、ステップS101に戻り、上述した処理を繰り返す。

#### 【0194】

また、ステップS111において、親機12-2のCPU111は、親機12-1からエラー通知を受信したと判定した場合、即ち、親機12-1がリソース利用条件文を発行せず、移動端末装置11-2によるリソース利用を許可しなかった場合、処理を終了する。

#### 【0195】

図11は、電子証明書の例を示す図である。

#### 【0196】

この電子証明書は、図11に示されるように、証明書のバージョン番号、証明書の通し番号、署名に用いたアルゴリズムとパラメータ、認証装置13の名前、証明書の有効期限、発行された装置のID、および装置の公開鍵が含まれている。

#### 【0197】

この電子証明書は、認証装置13により、親機12-1、親機12-2、およびバリュ発行装置14に対して発行される。親機12-1、親機12-2、およびバリュ発行装置14は、自らの正当性を証明するために他の装置に、暗号文とともにこの電子証明書を送信する。受信した装置は、この電子証明書に含まれる装置の公開鍵を用いて、この電子証明書とともに送信されてくる暗号文を復号し、その暗号文の正当性を認識することができる。

#### 【0198】

図12は、図6の親機12-1がリソース情報を送信する処理を説明するフロ

ーチャートである。この処理は、例えば、親機 12-1 が図 5 のステップ S 4 1 で移動端末装置 11-2 から送信されるブロードキャスト要求信号を受信したとき開始される。

#### 【0199】

ステップ S 120 において、親機 12-1 の CPU 9 1 は、移動端末装置 11-2 によるブロードキャスト要求を許可するかどうかを判定する。ステップ S 120 において、親機 12-1 の CPU 9 1 は、ブロードキャスト要求を許可すると判定した場合、ステップ S 121 に進み、移動端末装置 11-2 にブロードキャスト要求許可の通知を送信する。

#### 【0200】

ステップ S 121 の処理後は、ステップ S 122 に進み、親機 12-1 の CPU 9 1 は、移動端末装置 11-2 から図 5 のステップ S 4 3 でリソース情報要求信号が送信されて来るのを待って受信し、ステップ S 123 に進む。

#### 【0201】

ステップ S 123 において、親機 12-1 の CPU 9 1 は、入出力部 9 7 を制御し、データバス 9 8 とリソース制御部 9 9 を介して、リソース機器 15-1 とリソース機器 15-2 から、移動端末装置 12-2 に提供することができる、または提供してもよいリソースのリソース情報を取得する。同様に、CPU 9 1 は、入出力部 9 7 を制御し、データバス 9 8 を介して、リソース機器 16-1 とリソース機器 16-2 からリソース情報を取得する。そして、CPU 9 1 は、取得したリソース情報を移動端末装置 11-2 に送信して処理を終了する。

#### 【0202】

一方、ステップ S 120 において、CPU 9 1 は、移動端末装置 11-2 からのブロードキャスト要求を許可しないと判定した場合、ステップ S 124 に進み、移動端末装置 11 にブロードキャスト要求を許可しないことを示すエラー通知を送信し、処理を終了する。

#### 【0203】

図 13 は、図 6 の親機 12-1 が、リソース利用条件文を発行するときに行うリソース利用条件文発行処理を説明するフローチャートである。この処理は、親

機 12-1 が図 10 のステップ S100 の処理で親機 12-2 から送信された、暗号化された利用権発行要求文と電子証明書を受信したとき開始される。なお、親機 12-1 は、認証装置 13 から発行された電子証明書（図 11）を既に受信し、RAM 113 に保持しているものとする。

#### 【0204】

ステップ S141 において、親機 12-1 の CPU 111 は、親機 12-2 から利用権発行要求文とともに受信した電子証明書から公開鍵 40 を取得し、ステップ S142 に進む。ステップ S142 では、親機 12-1 の CPU 111 は、親機 12-2 から受信した利用権発行要求文から秘密鍵 38 を用いて暗号化された電子署名を取得する。CPU 111 は、暗号/復号部 117 を制御して、電子署名を、ステップ S141 で取得した、秘密鍵 38 と対の公開鍵 40 を用いて復号する。

#### 【0205】

ステップ S142 の処理後は、ステップ S143 に進み、親機 12-1 の CPU 111 は、利用権発行要求文が正当であるかどうかを判定する。即ち、親機 12-1 の CPU 111 は、ステップ S142 で電子署名が正常に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵 38 で暗号化された電子署名が、秘密鍵 38 に対応する公開鍵 40 で正常に復号されているので、親機 12-1 と親機 12-2 が通信する間で改ざんが行われていないと認識し、利用権発行要求文が正当であると判定する。

#### 【0206】

ステップ S143 において、親機 12-1 の CPU 111 は、利用権発行要求文が正当ではないと判定した場合、リソース利用を許可することはできないので、ステップ S148 に進み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

#### 【0207】

ステップ S143 において、親機 12-1 の CPU 111 は、利用権発行要求文が正当であると判定した場合、ステップ S144 に進み、親機 12-2 から受信した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置 13 に送信し、ステップ S145 に進む。

## 【0208】

ステップS145では、親機12-1のCPU111は、認証装置13から、図18のステップS183またはステップS184で送信される電子証明書の評価を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の評価を受信するまで待機する。

## 【0209】

ステップS145において、親機12-1のCPU111は、認証装置13から電子証明書の対価を受信したと判定した場合、ステップS146に進み、その認証装置13からの電子証明書の評価が有効であるかどうかを判定する。ステップS146において、親機12-1のCPU111は、認証装置13から電子証明書は有効であるという評価を受信したと判定した場合、即ち、利用件発行要求とともに送信されてきた電子証明書が失効していない（無効でない）場合、ステップS147に進み、リソース利用を許可するための対価を記載したリソース利用条件文を電子的に作成する。

## 【0210】

このとき、親機12-1のCPU111は、暗号/復号部117を制御して、自らの正当性を証明するために、秘密鍵35を用いて電子署名を暗号化し、リソース利用条件文に電子署名を付加する。そして、CPU111は、電子署名を付加した利用条件文と、RAM113に保持した電子証明書を、親機12-2に送信し、処理を終了する。

## 【0211】

一方、ステップS146において、親機12-1のCPU111は、認証装置13から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップS148に進み、リソース利用の不許可を示すエラー通知を親機12-2に送信し、処理を終了する。

## 【0212】

なお、親機12-1がリソースを利用する権利を記載した権利文を発行する処理も、図13と同様にして行われる。但し、この権利文を発行する処理は、バリ

ユー発行装置 14 から、後述する図 16 のステップ S 168 で送信される暗号化された振込み通知書と電子証明書を受信したとき開始される。

#### 【0213】

即ち、図 14 は、図 6 の親機 12-1 がリソースを利用するための権利文を発行するときに行う権利文発行処理を説明するフローチャートである。この処理は、親機 12-1 が後述する図 16 のステップ S 168 の処理でバリュ発行装置 14 から送信される、振込み通知書と電子証明書を受信したとき開始される。なお、親機 12-1 は、認証装置 13 から発行された電子証明書（図 11）を既に受信し、RAM 113 に保持しているものとする。

#### 【0214】

ステップ S 151 において、親機 12-1 の CPU 111 は、バリュ発行装置 14 から、振り込み通知書とともに受信した電子証明書から公開鍵 41 を取得し、ステップ S 152 に進む。ステップ S 152 では、親機 12-1 の CPU 111 は、バリュ発行装置 14 から受信した振込み通知書から秘密鍵 43 を用いて暗号化された電子署名を取得する。親機 12-1 の CPU 111 は、暗号/復号部 117 を制御して、電子署名を、ステップ S 151 で取得した公開鍵 41 を用いて復号する。

#### 【0215】

ステップ S 152 の処理後は、ステップ S 153 に進み、親機 12-1 の CPU 111 は、振込み通知書が正当であるかどうかを判定する。即ち、CPU 111 は、電子署名が正常に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵 43 で暗号化された電子署名が、秘密鍵 43 に対応する公開鍵 41 で正常に復号されているので、親機 12-1 とバリュ発行装置 14 が通信する間で改ざんが行われていないと認識し、振込み通知書が正当であると判定する。

#### 【0216】

ステップ S 153 において、親機 12-1 の CPU 111 は、振込み通知書が正当ではないと判定した場合、リソース利用を許可することはできないので、ステップ S 158 に進み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

## 【0217】

また、ステップS153において、親機12-1のCPU111は、振込み通知書が正当であると判定した場合、ステップS154に進み、バリュー発行装置14から受信した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置13に送信し、ステップS155に進む。

## 【0218】

ステップS155では、親機12-1のCPU111は、認証装置13から、後述する図18のステップS183またはステップS184で送信される電子証明書の評価を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の評価を受信するまで待機する。

## 【0219】

そして、ステップS155において、親機12-1のCPU111は、認証装置13から電子証明書の評価を受信したと判定した場合、ステップS156に進み、CPU111は、認証装置13から電子証明書は有効であるという評価を受信したかどうかを判定する。ステップS156において、CPU111は、認証装置13から電子証明書は有効であるという評価を受信したと判定した場合、ステップS157に進み、リソースを利用する権利を記載した権利文を電子的に作成する。このとき、親機12-1のCPU111は、暗号/復号部117を制御して、自らの正当性を証明するために、秘密鍵35を用いて電子署名を暗号化し、権利文に電子署名を付加する。そして、親機12-1のCPU111は、電子署名を付加した権利文と、RAM113に保持した電子証明書を、親機12-2に送信して処理を終了する。

## 【0220】

一方、ステップS156において、親機12-1のCPU111は、認証装置13から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップS158に進み、リソース利用の不許可を示すエラー通知を親機12-2に送信して処理を終了する。

## 【0221】

図15は、図1のバリュ発行装置14の詳細構成例である。

#### 【0222】

バリュ発行装置14は、通信部131、データバス132、共通秘密鍵認証部133、公開鍵認証部134、バリュ発行部135、共通秘密鍵記憶部136、秘密鍵記憶部137、証明書記憶部138、発行履歴記憶部139、およびバリュ記憶部140から構成されている。

#### 【0223】

通信部131は、インターネット21を介して、親機12-1、親機12-2、および認証装置13からの信号を受信するとともに、親機12-1、親機12-2、および認証装置13に信号を送信する。通信部131は、データバス132を介して、共通秘密鍵認証部133、公開鍵認証部134、およびバリュ発行部135に接続されている。

#### 【0224】

共通秘密鍵認証部133は、共通秘密鍵記憶部136に記憶された共通秘密鍵44に基づいて、バリュ発行装置14にアクセスしてきた親機12が正当であるかどうかを判定する。また、共通秘密鍵認証部133は、バリュ発行装置14がバリュを管理する親機12に対して、共通秘密鍵44と同一の秘密鍵34または37を送信し、親機12の非接触ICカード121に記憶させる。

#### 【0225】

このように、親機12の非接触ICカード121にバリュ発行装置14の共通秘密鍵44と等しい共通秘密鍵34または37を記憶させることにより、親機12とバリュ発行装置14との間での認証が可能となり、ユーザが、その親機12と通信が可能な移動端末装置11を使用するだけで、バリュ発行装置14を介して、親機12どうしの間でのバリュの移動をすることができる。

#### 【0226】

公開鍵認証部134は、秘密鍵記憶部137に記憶された秘密鍵43や、証明書記憶部138に記憶された電子証明書を用いて、親機12-1、親機12-2、および認証装置13との間で通信部131を開始、公開鍵暗号系の処理を行う。



**【0227】**

バリュー発行部 135 は、バリュー記憶部 140 に記憶されたバリュー（電子バリュー）に基づき、バリューを発行し、その発行履歴を発行履歴記憶部 139 に記憶させる。

**【0228】**

なお、バリュー発行装置 14 は、物理的に 1 つの筐体に入る必要はなく、データバス 132 を経由して複数の機器が協調して機能を実現してもよい。

**【0229】**

また、バリュー発行装置 14 は、発行したバリューに応じた対価を決済できるようにしてもよい。さらに、親機 12 は、所有する電子バリューをネットワークでの決済に使用してもよい。

**【0230】**

また、電子バリューの形式は何でもよい。電子バリューはバリュー発行装置 14 のバリュー記憶部 140 に口座という形で格納してもよい。この場合、より高い安全性を提供することができる。

**【0231】**

さらに、バリューは、バリュー発行装置 14 のバリュー記憶部 140 に口座という形で記憶されるだけでなく、親機 12 の安全なデバイス（例えば、非接触 IC カード 121）の記憶領域へ格納されてもよい。この場合、バリュー発行装置 14 のバリュー発行部 135 で発行された電子バリューは、親機 12 の非接触 IC カード 121 に転送される。例えば、バリュー発行装置 14 が、親機 12-2 から親機 12-1 に対してバリューを振り込む場合、バリュー発行装置 14 は、親機 12-2 からバリューを取得し、バリューを親機 12-1 に送信する。なお、バリューの送受信は、バリューを暗号化して安全に行われる。

**【0232】**

また、バリューは、バリュー発行装置 14 のバリュー記憶部 140 および親機 12 の安全なデバイスの両者の組み合わせによって記憶されてもよい。この組み合わせとして、バリュー発行装置 14 は、ユーザの電子バリューをバリュー記憶部 140 の中でそれぞれのユーザの口座として記憶し、その口座を管理しつつ、

必要な額だけをユーザのデバイス（例えば、非接触 IC カード）へ移動させ財布のように利用させてもよい。

### 【0233】

図16は、図15のバリュー発行装置14が振り込み通知書を親機12-1に送信する処理を説明するフローチャートである。この処理は、バリュー発行装置14が、親機12-2が図10のステップS103で送信したバリュー移動要求を受信したとき開始される。なお、バリュー発行装置14は、認証装置13が発行した電子証明書を、既に証明書記憶部138に記憶しているものとする。

### 【0234】

ステップS161において、共通秘密鍵認証部133は、共通秘密鍵記憶部136から共通秘密鍵44と、秘密鍵記憶部137から秘密鍵43を読み出し、秘密鍵43を用いて、共通秘密鍵44を暗号化する。ステップS161の処理後は、ステップS162に進み、共通秘密鍵認証部133は、その暗号化された共通秘密鍵44を親機12-2に送信し、ステップS163に進む。即ち、共通秘密鍵認証部133は、暗号化された共通秘密鍵44を、データベース132を介して通信部131に供給し、通信部131は、その暗号化された共通秘密鍵44を親機12-2に送信する。

### 【0235】

ステップS163において、通信部131は、親機12-2から、図10のステップS109で送信された暗号化された共通秘密鍵37を受信したかどうかを判定する。ステップS163において、通信部131は、親機12-2から暗号化された共通秘密鍵37を受信していないと判定した場合、ステップS164に進み、親機12-2から、図10のステップS110で送信される、バリュー発行装置14と親機12-2の関係が正当ではないことを示すエラー通知を受信したかどうかを判定する。ステップS168において、通信部131は、エラー通知を受信していないと判定した場合、ステップS163に戻り、上述した処理を繰り返す。

### 【0236】

ステップS164において、通信部131は、エラー通知を受信したと判定し

た場合、バリユー発行装置 14 と親機 12-2 の関係が正当ではないので、バリユー移動の不許可を示すエラー通知を送信して処理を終了する。

#### 【0237】

一方、ステップ S163 において、通信部 131 は、親機 12-2 から暗号化された共通秘密鍵 37 を受信したと判定した場合、その暗号化された共通秘密鍵 37 を公開鍵認証部 134 に供給し、ステップ S163 からステップ S165 に進む。ステップ S165 において、公開鍵認証部 134 は、暗号化された共通秘密鍵 37 を、秘密鍵記憶部 137 に記憶している秘密鍵 43 を用いて復号する。

#### 【0238】

ステップ S165 の処理後は、ステップ S166 に進み、公開鍵認証部 134 は、共通秘密鍵認証部 133 に、ステップ S165 で復号した共通秘密鍵 37 を供給し、共通秘密鍵認証部 133 は、復号した共通秘密鍵 37 と共通秘密鍵記憶部 136 に記憶している共通秘密鍵 44 が等しいかどうかを判定する。

#### 【0239】

ステップ S166 において、共通秘密鍵認証部 133 は、復号した共通秘密鍵 37 と共通秘密鍵 44 が等しいと判定した場合、親機 12-2 とバリユー発行装置 14 の関係は正当であると認識して、ステップ S166 からステップ S167 に進む。即ち、この場合、親機 12-1 において公開鍵 41 を用いて暗号化された共通秘密鍵 37 が、バリユー発行装置 14 において、公開鍵 41 に対応する秘密鍵 43 を用いて正常に復号され、共通秘密鍵 37 が得られているので、バリユー発行装置 14 は、親機 12-2 とバリユー発行装置 14 が通信する間で改ざんが行われていないと認識する。

#### 【0240】

さらに、バリユー発行装置 14 は、親機 12-2 が有する共通秘密鍵 37 とバリユー発行装置 14 が有する共通秘密鍵 44 が等しいので、親機 12-2 がバリユーを管理することを認められている相手であることを認識する。即ち、バリユー発行装置 14 は、バリユー発行装置 14 の有する共通秘密鍵 44 と同一の秘密鍵 37 を、親機 12-2 に備えられる安全なデバイス（非接触 IC カード 121）に配布し、親機 12-2 が共通秘密鍵 44 と等しい共通秘密鍵 37 を有するこ

とを認識することによって、正しい親機 12-2 からのアクセスであることを認識する。

#### 【0241】

ステップ S167 において、バリュー発行部 135 は、親機 12-2 から親機 12-1 にバリューを移動する。即ち、バリュー発行部 135 は、バリュー記憶部 140 に記憶された親機 12-2 の所定の対価に対応するバリューを削除し、親機 12-1 のバリューに所定の対価に対応するバリューを追加し、これにより、親機 12-2 のユーザの電子バリューが、そのユーザが移動端末装置 11-2 によってリソースを利用しようとしている親機 12-1 のユーザに対し、そのリソースの利用に対する対価として振り込まれる。さらに、ステップ S167 では、バリュー発行部 135 は、バリューの移動完了を示す取引結果通知を生成する。

#### 【0242】

これにより、ユーザは、バリュー発行装置 14 を経由して、他のユーザとの間で、電子バリューの授受を行うことができる。

#### 【0243】

ステップ S167 の処理後は、ステップ S168 に進み、公開鍵認証部 134 は、秘密鍵記憶部 137 に記憶された秘密鍵 43 を用いて、自らの正当性を証明するために電子署名を暗号化する。そして、公開鍵認証部 134 は、その暗号化した電子署名を付加した振込み通知書を作成する。この振込み通知書は、バリューの振込みを知らせるための振込み通知と、バリューの振込みの詳細が記載されたレシートから構成されている。そして、公開鍵認証部 134 は、その振込み通知書、証明書記憶部 138 に記憶された電子証明書、および電子バリューの移動完了を示す取引結果通知を、バリューの振込先であるユーザの親機 12-1 に送信して処理を終了する。

#### 【0244】

一方、ステップ S166 において、共通秘密鍵認証部 133 は、ステップ S165 で復号した共通秘密鍵と共通秘密鍵 44 が等しくないと判定した場合、親機 12-2 とバリュー発行装置 14 の関係は正当ではないので、バリュー移動の不

許可を示すエラー通知を送信して処理を終了する。

#### 【0245】

図17は、図1の認証装置13の詳細構成例を示している。

#### 【0246】

認証装置13は、通信部151、データベース152、公開鍵認証部153、秘密鍵記憶部154、証明書記憶部155、公開鍵記憶部156、証明書記憶部157、および証明書失効リスト記憶部158から構成されている。

#### 【0247】

通信部151は、インターネット21を介して、親機12-1、親機12-2、およびバリュウ発行装置14から送信された信号を受信するとともに、親機12-1、親機12-2、およびバリュウ発行装置14に信号を送信する。通信部151は、データベース152を介して、公開鍵認証部153と接続されている。

#### 【0248】

公開鍵認証部153は、公開鍵記憶部156に記憶された公開鍵と、一般公開用証明書記憶部157に記憶された一般公開用証明書を公開したり、電子証明書を発行する。また、公開鍵認証部153は、電子証明書が有効であるかどうかを判定する。

#### 【0249】

秘密鍵記憶部154には、秘密鍵42が記憶される。証明書記憶部155には、認証装置13の電子証明書が記憶される。公開鍵記憶部156には、親機12-1の秘密鍵35に対応する公開鍵39、親機12-2の秘密鍵38に対応する公開鍵40、およびバリュウ発行装置14の秘密鍵43に対応する公開鍵41が記憶される。

#### 【0250】

一般公開用証明書記憶部157には、公開鍵認証部153が発行した一般公開用の電子証明書が記憶され、この電子証明書が親機12やバリュウ発行装置14に提供される。証明書失効リスト記憶部158には、失効した電子証明書を示す証明書失効リストが記憶される。即ち、一般公開用証明書記憶部157に記憶された電子証明書が何らかの理由により失効したとき、その電子証明書が、その証

明書失効リストにエントリされる。

#### 【0251】

図18は、図17の認証装置13が電子証明書の判定を行う処理を説明するフローチャートである。この処理は、親機12などから電子証明書の有効性の判定を要求する信号を受信したとき開始する。

#### 【0252】

ステップS181において、公開鍵認証部153は、証明書失効リスト記憶部158から、失効した電子証明書を示す証明書失効リストを読み出し、ステップS182に進む。ステップS182において、公開鍵認証部153は、親機12から受信した電子証明書の判定を要求する信号に基づいて、判定の対象となる電子証明書が失効しているかどうかを判定する。即ち、公開鍵認証部153は、ステップS181で読み出された証明書失効リストに、判定の対象となる電子証明書があるかどうかを判定する。

#### 【0253】

ステップS182において、公開鍵認証部153は、判定の対象となる電子証明書が失効していると判定した場合、ステップS183に進み、データバス152を介して通信部151から、親機12に電子証明書の無効通知を送信して処理を終了する。

#### 【0254】

ステップS182において、公開鍵認証部153は、判定の対象となる電子証明書が失効していないと判定した場合、ステップS184に進み、データバス152を介して通信部151から、親機12に電子証明書の有効通知を送信して処理を終了する。

#### 【0255】

図19は、図1の通信システム1の全体の処理を説明するフローチャートである。即ち、図19のフローチャートは、移動端末装置11-1と移動端末装置11-2が親機12-1とのみ直接無線通信することができる場合に、その親機12-1に接続されたりソース機器15-1を利用するときの通信システム全体の処理を示している。

## 【0256】

なお、図19では、移動端末装置11-1、移動端末装置11-2、親機12-1、親機12-1、認証装置13、およびバリュー発行装置14は、それぞれが通信する間で改ざんが行われず、正当な関係であるとする。

## 【0257】

また、図19では、まず最初に、移動端末装置11-1がその本親機である親機12-1にリソースを要求し、その後、移動端末装置11-2が、無線通信できるが本親機でない親機12-1にリソースを要求するものとする。

## 【0258】

ステップS231において、移動端末装置11-1は、その本親機である親機12-1と双方向認証するために、共通秘密鍵31を暗号化して、親機12-1に送信する。

## 【0259】

ステップS251において、親機12-1は、移動端末装置11-1から暗号化された共通秘密鍵31を受信する。ステップS252において、親機12-1は、共通秘密鍵33を暗号化し、移動端末装置11-1に送信する。

## 【0260】

ステップS232において、移動端末装置11-1は、親機12-1から暗号化された共通秘密鍵33を受信する。ステップS233において、移動端末装置11-1は、その暗号化された共通秘密鍵33を復号し、復号した共通秘密鍵33を暗号化して、暗号化した共通秘密鍵33を親機12-1に送信する。

## 【0261】

ステップS253において、親機12-1は、暗号化された共通秘密鍵33を、移動端末装置11-1から受信する。ステップS254において、親機12-1は、暗号化された共通秘密鍵33を復号する。親機12-1は、復号した共通秘密鍵33から、親機12-1と移動端末装置11-1の関係が正当であるかどうかを判定する。この例では、親機12-1と移動端末装置11-1は正当な関係であるので、親機12-1は、ステップS251で移動端末装置11-1から受信した暗号化された共通秘密鍵31を復号し、その復号した共通秘密鍵31を

暗号化して、移動端末装置 11-1 に送信する。

【0262】

ステップ S234 において、移動端末装置 11-1 は、親機 12-1 から暗号化された共通秘密鍵 31 を受信し、その暗号化された共通秘密鍵 31 を復号する。移動端末装置 11-1 は、復号した共通秘密鍵 31 から、親機 12-1 と移動端末装置 11-1 の関係が正当であるかどうかを判定する。この例では、親機 12-1 と移動端末装置 11-1 の関係は正当であるので、双方向認証を完了し、ステップ S235 において、移動端末装置 11-1 は、リソースを要求する信号を親機 12-1 に送信する。

【0263】

即ち、移動端末装置 11-1 は、その本親機である親機 12-1 と双方向認証することにより、移動端末装置 11-1 を使用するユーザが正しいユーザであることを、通信システム 1 のユーザに保証する。

【0264】

ステップ S255 において、親機 12-1 は、移動端末装置 11-1 からリソースを要求する信号を受信する。ステップ S256 において、親機 12-1 は、リソースを要求する信号に基づいて、要求対象となるリソース機器 15-1 にリソースを要求する信号を送信する。

【0265】

ステップ S291 において、リソース機器 15-1 は、親機 12-1 からリソースを要求する信号を受信する。ステップ S292 において、リソース機器 15-1 は、リソースを要求する信号に基づいて、要求対象となるリソースを親機 12-1 を介して、移動端末装置 11-1 に送信する。

【0266】

ステップ S236 において、移動端末装置 11-1 は、リソース機器 15-1 から親機 12-1 を介して、リソースを受信し、これにより、リソース機器 15-1 を利用することが可能な状態となる。

【0267】

一方、移動端末装置 11-2 は、ステップ S201 において、リソース情報を



取得するために、その本親機でない親機 12-1 にブロードキャストを要求する信号を送信する。

**【0268】**

ステップ S257 において、親機 12-1 は、移動端末装置 11-2 からブロードキャストを要求する信号を受信し、ブロードキャスト要求を許可するかどうかを判定する。図 19 では、ステップ S258 において、親機 12-1 は、ブロードキャストを許可し、ブロードキャストを許可する信号を、移動端末装置 11-2 に送信する。

**【0269】**

ステップ S202 において、移動端末装置 11-2 は、親機 12-1 からブロードキャストを許可する信号を受信する。ステップ S203 において、移動端末装置 11-2 は、親機 12-1 が取得できるリソースの情報（親機 12-1 が、移動端末装置 11-2 に提供することができるリソースの情報）を要求する信号を、親機 12-1 に送信する。

**【0270】**

ステップ S259 において、親機 12-1 は、移動端末装置 11-2 からリソースの情報を要求する信号を受信する。ステップ S260 において、親機 12-1 は、リソース情報を移動端末装置 11-2 に送信する。

**【0271】**

ステップ S204 において、移動端末装置 11-2 は、親機 12-1 からリソース情報を受信する。ステップ S205 において、移動端末装置 11-2 は、親機 12-2 と双方向認証をするため、共通秘密鍵 32 を暗号化し、その暗号化した共通秘密鍵 32 を親機 12-2 に送信する。

**【0272】**

ステップ S311 において、親機 12-2 は、移動端末装置 11-2 から、暗号化された共通秘密鍵 32 を受信する。ステップ S312 において、親機 12-2 は、共通秘密鍵 36 を暗号化し、暗号化した共通秘密鍵 36 を移動端末装置 11-2 に送信する。

**【0273】**

ステップS206において、移動端末装置11-2は、親機12-2から暗号化した共通秘密鍵36を受信し、暗号化した共通秘密鍵36を復号する。移動端末装置11-2は、復号した共通秘密鍵36から、移動端末装置11-2と親機12-2の関係が正当であるかどうかを判定する。この例の場合、移動端末装置11-2と親機12-2の関係は正当であるので、ステップS207において、移動端末装置11-2は、復号した共通秘密鍵36を暗号化し、暗号化した共通秘密鍵36を親機12-2に送信する。

#### 【0274】

ステップS313において、親機12-2は、移動端末装置11-2から暗号化した共通秘密鍵36を受信し、その暗号化した共通秘密鍵36を復号する。親機12-2は、復号した共通秘密鍵36から、親機12-2と移動端末装置11-2の関係は正当であるかどうかを判定する。この例の場合、親機12-2と移動端末装置11-2の関係は正当であるので、ステップS314において、親機12-2は、ステップS311で移動端末装置11-2から受信した暗号化された共通秘密鍵32を復号し、復号した共通秘密鍵32を暗号化する。親機12-2は、その暗号化した共通秘密鍵32を移動端末装置11-2に送信する。

#### 【0275】

ステップS208において、移動端末装置11-2は、親機12-2から暗号化された共通秘密鍵32を受信し、その暗号化された共通秘密鍵32を復号する。移動端末装置11-2は、復号した共通秘密鍵32から、移動端末装置11-2と親機12-2の関係が正当であるかどうかを判定する。この例では、移動端末装置11-2と親機12-2の関係が正当であるので、双方向認証を完了し、ステップS209において、移動端末装置11-2は、リソースを要求する信号を親機12-2に送信する。

#### 【0276】

ステップS315において、親機12-2は、移動端末装置11-2から、リソースを要求する信号を受信する。ステップS316において、親機12-2は、親機12-1にリソース情報の識別子と利用方法を明記した利用権発行要求と電子証明書を、親機12-1に送信する。

## 【0277】

ステップS261において、親機12-1は、親機12-2から利用権発行要求と電子証明書を受信する。ステップS262において、親機12-1は、その電子証明書が有効であるかどうかの判定要求を認証装置13に送信する。

## 【0278】

ステップS361において、認証装置13は、親機12-1から電子証明書の判定要求を受信し、その電子証明書が有効であるかどうかを判定する。なお、ここでは、電子証明書は有効であるものとし、ステップS362において、認証装置13は、親機12-1に対象の電子証明書が有効であることを示す信号を送信する。

## 【0279】

ステップS263において、親機12-1は、認証装置13から電子証明書が有効であることを示す信号を受信する。ステップS264において、親機12-1は、リソースの利用を許可するための対価を記載したリソース利用条件文と電子証明書を、親機12-2に送信する。

## 【0280】

ステップS317において、親機12-2は、親機12-1からリソース利用条件文と電子証明書を受信する。ステップS318において、親機12-2は、バリュウ発行装置14にバリュウ移動要求を送信する。

## 【0281】

ステップS341において、バリュウ発行装置14は、親機12-2からバリュウ移動要求を受信する。ステップS342において、バリュウ発行装置14は、親機12-2と双方向認証するため、共通秘密鍵44を暗号化して、暗号化した共通秘密鍵44を親機12-2に送信する。

## 【0282】

ステップS320において、親機12-2は、バリュウ発行装置14から、暗号化された共通秘密鍵44を受信し、その暗号化された共通秘密鍵44を復号する。親機12-2は、復号した共通秘密鍵44から、親機12-2とバリュウ発行装置14の関係が正当であるかどうかを判定する。この例の場合、親機12-

2 とバリュウ発行装置 14 の関係は正当であるので、ステップ S 320 において、親機 12-2 は、共通秘密鍵 37 を暗号化し、暗号化した共通秘密鍵 37 をバリュウ発行装置 14 に送信する。

#### 【0283】

ステップ S 343 において、バリュウ発行装置 14 は、親機 12-2 から暗号化された共通秘密鍵 37 を受信し、その暗号化された共通秘密鍵 37 を復号する。バリュウ発行装置 14 は、復号した共通秘密鍵 37 から、バリュウ発行装置 14 と親機 12-2 の関係が正当であるかどうかを判定する。この例の場合、バリュウ発行装置 14 と親機 12-2 の関係は正当であるので、ステップ S 344 において、バリュウ発行装置 14 は、ステップ S 341 で受信したバリュウ移動要求に応じてバリュウを移動し、即ち、ここでは、親機 12-1 のユーザから親機 12-1 のユーザにバリュウを移動し、バリュウが移動されたことを示す振込み通知と電子証明書を、親機 12-1 に送信する。

#### 【0284】

ステップ S 265 において、親機 12-1 は、バリュウ発行装置 14 から、振込み通知書と電子証明書を受信する。ステップ S 266 において、親機 12-1 は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置 13 に送信する。

#### 【0285】

ステップ S 363 において、認証装置 13 は、親機 12-1 から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機 12-2 の電子証明書は有効であるので、ステップ S 364 において、認証装置 13 は、親機 12-1 に対象の電子証明書が有効であることを示す信号を送信する。

#### 【0286】

ステップ S 267 において、親機 12-1 は、認証装置 13 から電子証明書が有効であることを示す信号を受信する。ステップ S 268 において、親機 12-1 は、リソースを利用する権利を記載した権利文を発行し、その権利文と電子証明書を親機 12-2 に送信する。

## 【0287】

ステップS321において、親機12-2は、親機12-1から送信されてくる権利文と電子証明書を受信する。ステップS322において、親機12-2は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置13に送信する。

## 【0288】

ステップS365において、認証装置13は、親機12-2から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機12-1の電子証明書は有効であるので、ステップS366において、認証装置13は、親機12-2に対象の電子証明書が有効であることを示す信号を送信する。

## 【0289】

ステップS323において、親機12-2は、認証装置13から電子証明書が有効であることを示す信号を受信する。ステップS324において、親機12-2は、ステップS321で、親機12-1から受信した権利文を、移動端末装置11-2に送信する。

## 【0290】

ステップS210において、移動端末装置11-2は、親機12-1から権利文を受信する。ステップS211において、移動端末装置11-2は、その権利文とリソースを要求する信号を、親機12-1に送信する。

## 【0291】

ステップS269において、親機12-1は、移動端末装置11-2から、権利文とリソースを要求する信号を受信する。ステップS270において、親機12-1は、リソース機器15-1にリソースを要求する信号を送信する。

## 【0292】

ステップS293において、リソース機器15-1は、親機12-1からリソースを要求する信号を受信する。ステップS294において、リソース機器15-1は、親機12-1から要求されたリソースを親機12-1を介して、移動端末装置11-2に送信する。

## 【0293】

ステップ S 2 1 2 において、リソース機器 1 5 - 1 から、リソースを受信する。

## 【0294】

以上により、移動端末装置 1 1 - 2 は、親機 1 2 - 1 から権利文を取得することにより、親機 1 2 - 1 に接続されたリソース機器 1 5 - 1 を利用できる環境を得ることができる。

## 【0295】

以上のように、通信システム 1 では、バリュー発行装置 1 4 は、バリューの管理をする親機 1 2 に対して共通秘密鍵 4 4 と同一の秘密鍵 3 4 や 3 7 を送信し、親機 1 2 の非接触 IC カード 1 2 1 に記憶させる。親機 1 2 は、個人情報に格納するユーザに、親機 1 2 と通信可能にするための共通秘密鍵を格納した非接触 IC カード 7 1 を発行する。これにより、ユーザは、非接触 IC カード 7 1 の情報を移動端末装置 1 1 に読み込ませるだけで、本親機である親機 1 2 と通信をし、バリューの移動をすることができる。そして、ユーザは、上述した一連の処理を、例えば、非接触 IC カード 7 1 を移動端末装置 1 1 に、ワンタッチすることで行わせることができ、この場合、利便性の高い付加価値を提供することができる。

## 【0296】

さらに、認証情報やそれに伴うユーザの個人情報を管理する本親機となる親機 1 2 を、例えばユーザ宅のホームサーバという形で、移動端末装置 1 1 とは別に設けたので、ユーザと移動端末装置 1 1 とは依存関係がなく、リソースの利用時にのみユーザの認証を行えば済む。また、ユーザは、個人情報をバリュー発行装置に管理させることなく、自らの所有する親機 1 2 に格納し、バリューの決済情報だけを親機 1 2 とバリュー発行装置 1 4 との間でやりとりするだけで済む。さらに、ユーザが移動する場合においても、ユーザは、移動した空間にある機器（リソース）を、匿名のままユーザの嗜好に合わせた操作性で操作することができる。

## 【0297】

また、図1の通信システム1によれば、ユーザが、移動した空間にある移動端末装置11-2を操作することにより、そのユーザが個人情報管理する親機（本親機）12-2が、バリュー発行装置14の仲介の下、他人の親機12-1に電子バリューを支払って、その親機12-1のリソースの利用権を入手し、その利用権を、移動端末装置11-2が受け取って、親機12-1に提示することで移動端末装置11-2のユーザは、他人の親機12-1のリソースを、匿名のまま利用することができる。即ち、バリュー発行装置14は、移動端末装置11-2のユーザの親機12-2から他人の親機12-1に対しての電子バリューの振込みを仲介するだけであり、ユーザの個人情報の管理は、親機12で行われる。従って、電子バリューの決済の場と、個人情報の管理の場とが完全に分離されているといえることができる。なお、移動端末装置11-2からバリュー発行装置14にアクセスし、電子バリューを、リソースを利用しようとする親機12-1に振込み、移動端末装置11-2から親機12-1のリソースを利用することも可能である。但し、この場合、親機12-1に対する、移動端末装置11-2のユーザの匿名性は確保されるが、移動端末装置11-2のユーザの個人情報の管理は、移動端末装置11-2がアクセスするバリュー発行装置14で行われることになる。

#### 【0298】

さらに、移動端末装置11-2は、リソースを利用する親機12-1を介して、本親機である親機12-2にアクセスして、そのリソースの利用権を取得するので、利用したいリソースに近い位置で、その利用権を得ることができる。

#### 【0299】

ここで、移動端末装置11としては、例えば、PDA(Personal Digital Assistant)や、携帯用コンピュータ、携帯電話機、腕時計、デジタルスチルカメラ、デジタルビデオカメラなどの携帯性に優れた装置を採用することが可能である。

#### 【0300】

また、出先のユーザが移動端末装置11から利用するリソースとしては、例えば、「装置」や、「情報」、「情報に対するライセンス」などがある。

#### 【0301】

リソースとしての「装置」には、例えば、無線アクセスポイントや、テレビジョン受像機、電話機などが含まれる。リソースとして「装置」を利用するケースとしては、例えば、出先のユーザが、移動端末装置 11 から、他人の無線アクセスポイントを利用してインターネットに接続する場合がある。

#### 【0302】

また、リソースとしての「情報」には、いわゆるホームサーバやチャンネルサーバなどで構成される親機 12-1 が管理するコンテンツその他の情報などが含まれる。リソースとして「情報」を利用するケースとしては、例えば、出先のユーザが、親機 12-1 としてのチャンネルサーバに蓄えられたコンテンツを視聴する場合がある。

#### 【0303】

さらに、リソースとしての「情報に対するライセンス」には、情報が暗号化されている場合に、その暗号化を解くための鍵などが含まれる。リソースとして「情報に対するライセンス」を利用するケースとしては、例えば、携帯端末装置 11 に、ネットワーク経由でダウンロードした、暗号化されたコンテンツを視聴する場合に、そのコンテンツを視聴するためのライセンスとしての暗号鍵を取得するときなどがある。

#### 【0304】

なお、上述した一連の処理では、移動端末装置 11-1 と移動端末装置 11-2 のユーザは異なっていたが、同一ユーザの親機や移動端末装置間でも同様に電子バリューの移動をすることができる。

#### 【0305】

なお、本明細書において、フローチャートに記載された処理は、ステップとして記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

#### 【0306】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。



## 【0307】

## 【発明の効果】

以上の如く、本発明によれば、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作させることができる。また、そのとき発生する対価の支払いを自動的に行うことができる。さらに、利便性がよく、安全な通信をすることができる。

## 【図面の簡単な説明】

## 【図1】

本発明を適用した通信システムの構成例を示すブロック図である。

## 【図2】

図1の移動端末装置の構成例を示すブロック図である。

## 【図3】

図2の移動端末装置におけるリソース取得処理を説明するフローチャートである。

## 【図4】

図3のステップS2およびステップS6の共通秘密鍵認証処理を説明するフローチャートである。

## 【図5】

図3のステップS5のリソース情報取得処理を説明するフローチャートである。

## 【図6】

図1の親機の構成例を示す図である。

## 【図7】

図6のリソース制御部の構成例を示す図である。

## 【図8】

図6の親機におけるリソース制御処理を説明するフローチャートである。

## 【図9】

図8のステップS71のリソース送信処理を説明するフローチャートである。

## 【図10】

図 8 のステップ S 7 1 のリソース送信処理を説明するフローチャートである。

【図 1 1】

電子証明書の例を示す図である。

【図 1 2】

図 6 の親機におけるリソース情報送信処理を説明する図である。

【図 1 3】

図 6 の親機におけるリソース利用条件文発行処理を説明するフローチャートである。

【図 1 4】

図 6 の親機における権利文発行要求処理を説明するフローチャートである。

【図 1 5】

図 1 のバリュウ発行装置の構成例を示す図である。

【図 1 6】

図 1 5 のバリュウ発行装置における振込み通知書送信処理を説明するフローチャートである。

【図 1 7】

図 1 の認証装置の構成例を示す図である。

【図 1 8】

図 1 7 の認証装置における電子証明書判定処理を説明する図である。

【図 1 9】

図 1 の通信システムにおけるリソース取得処理を説明する図である。

【符号の説明】

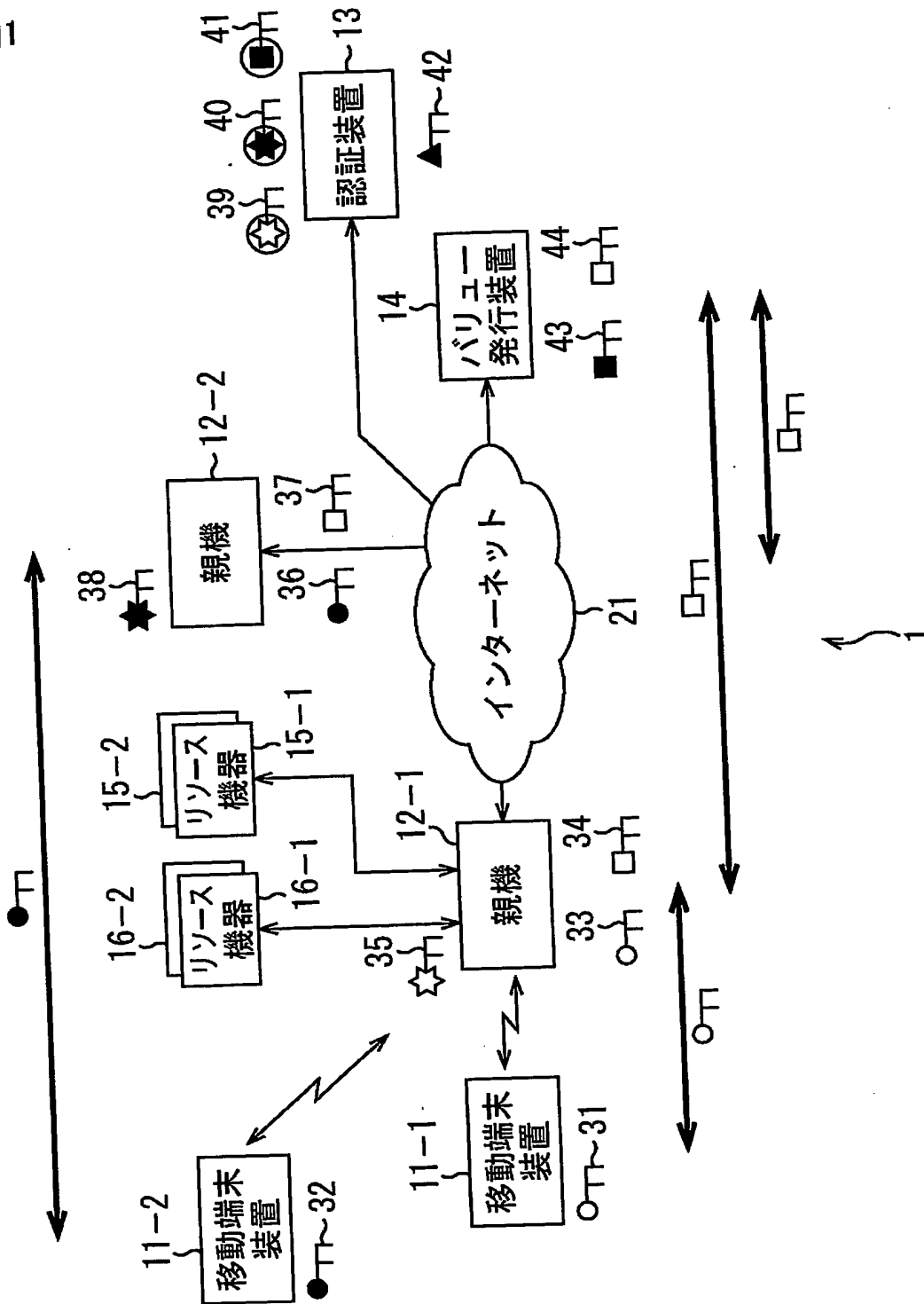
1 1 移動端末装置, 1 2 親機, 1 3 認証装置, 1 4 バリュウ発行装置, 1 5 リソース, 1 6 リソース, 2 1 インターネット, 3 1 共通秘密鍵, 3 2 共通秘密鍵, 3 3 共通秘密鍵, 3 4 共通秘密鍵, 3 5 秘密鍵, 3 6 共通秘密鍵, 3 7 共通秘密鍵, 3 8 秘密鍵, 3 9 公開鍵, 4 0 公開鍵, 4 1 公開鍵, 4 2 秘密鍵, 4 3 秘密鍵, 4 4 共通秘密鍵, 6 9 暗号/復号部 7 1 非接触 IC カード, 1 2 1 非接触 IC カード, 1 1 7 暗号/復号部 1 3 3 共通秘

密鍵認証部, 134 公開鍵認証部, 135 バリユー発行部, 153  
公開鍵認証部, 158 証明書失効リスト記憶部

【書類名】 図面

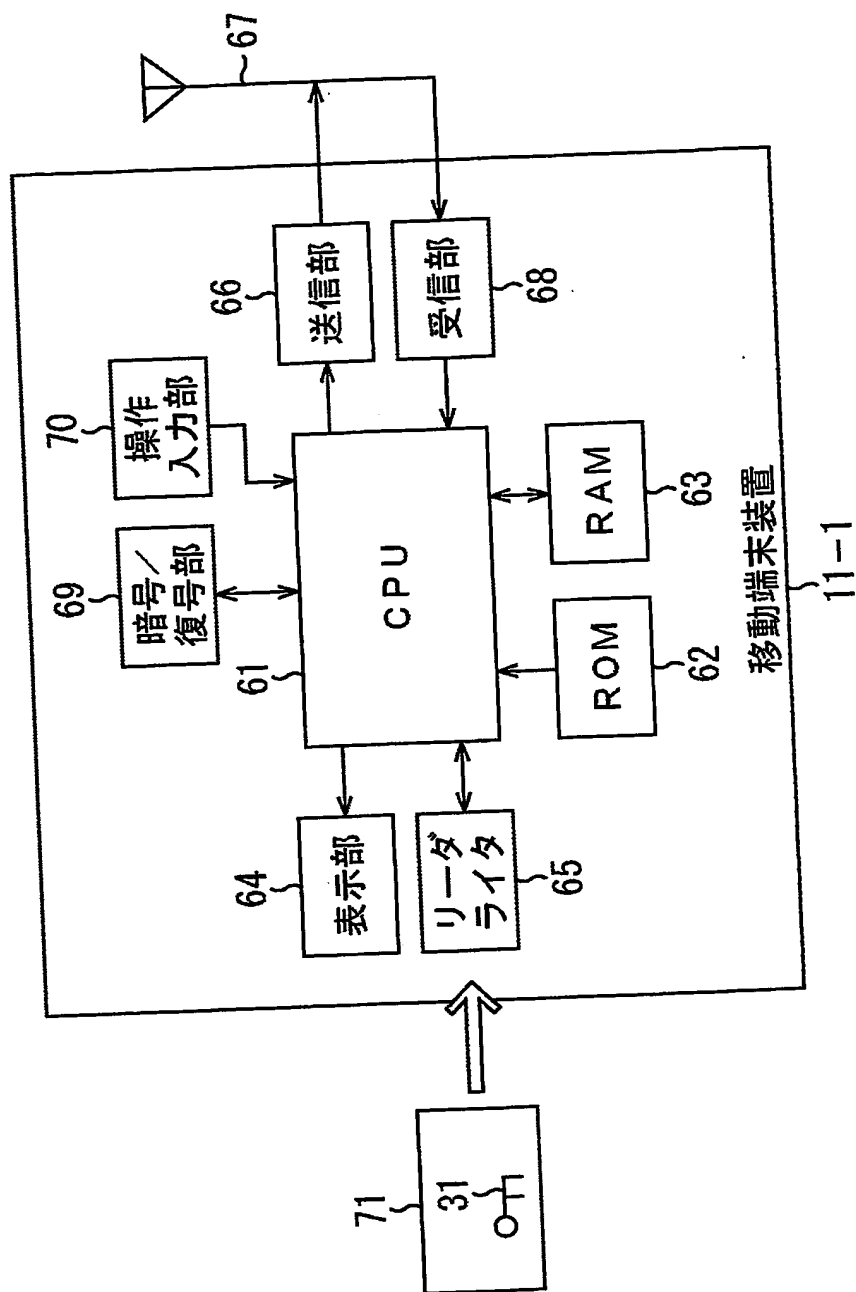
【図 1】

図1



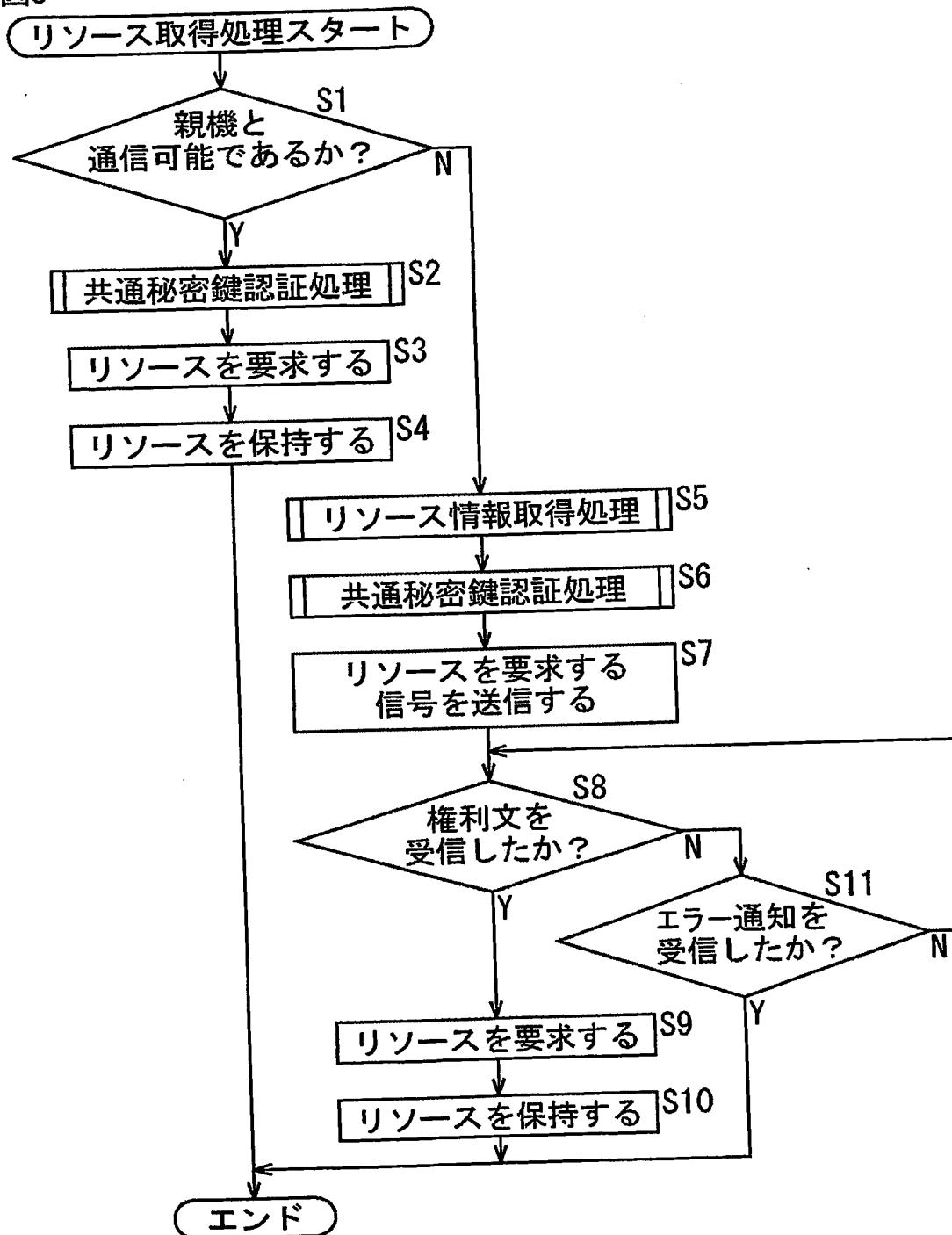
【図 2】

図2



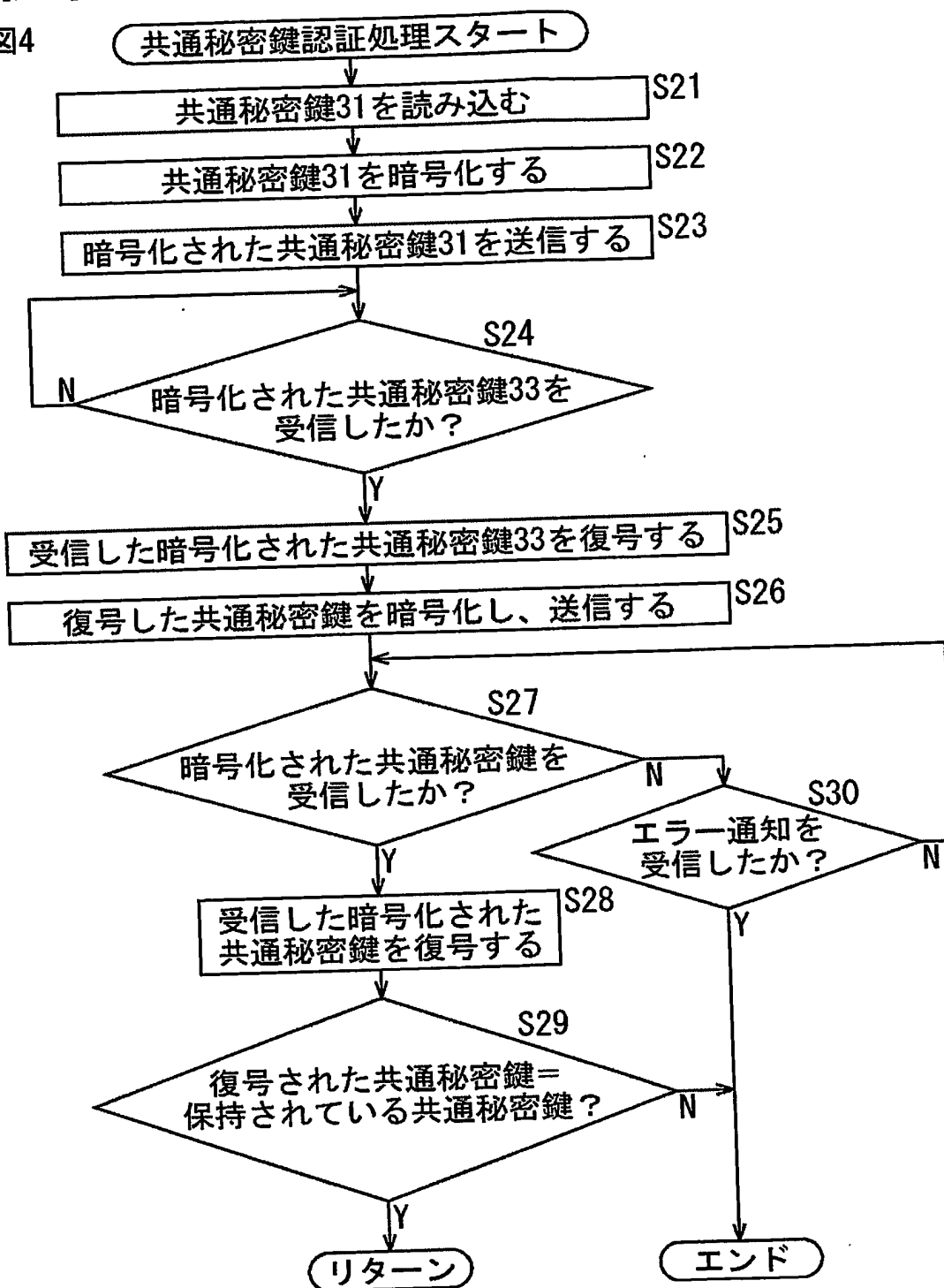
【図 3】

図3



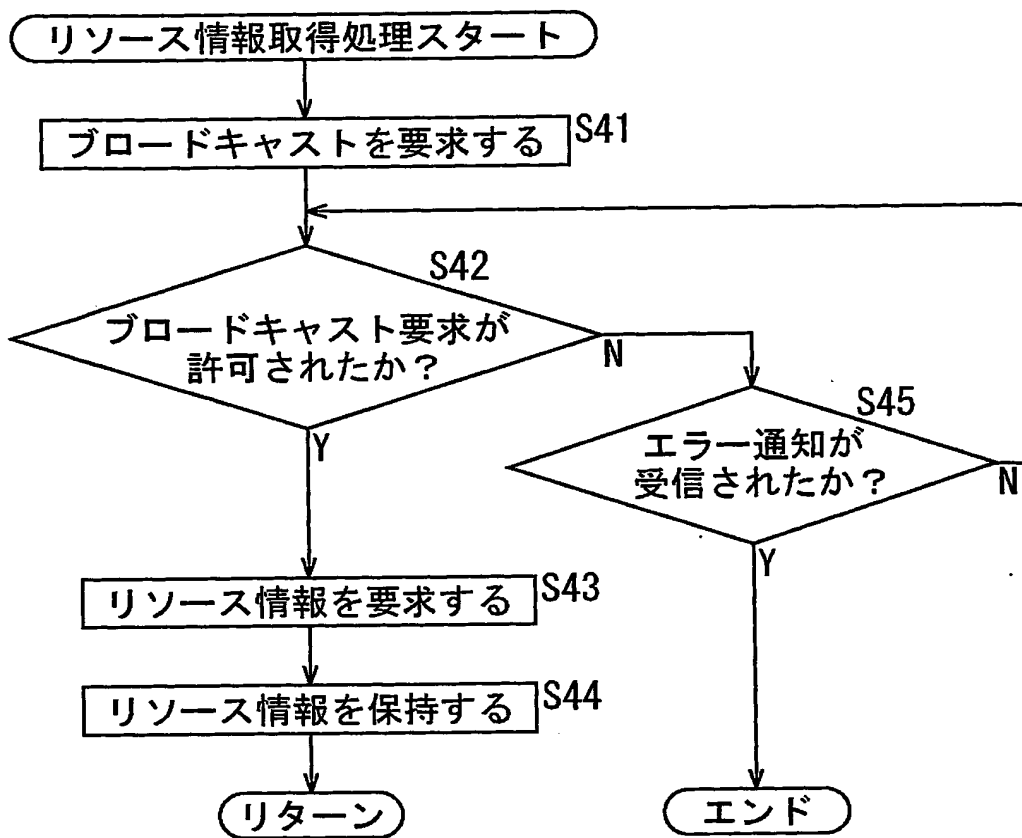
【図 4】

図4



【図 5】

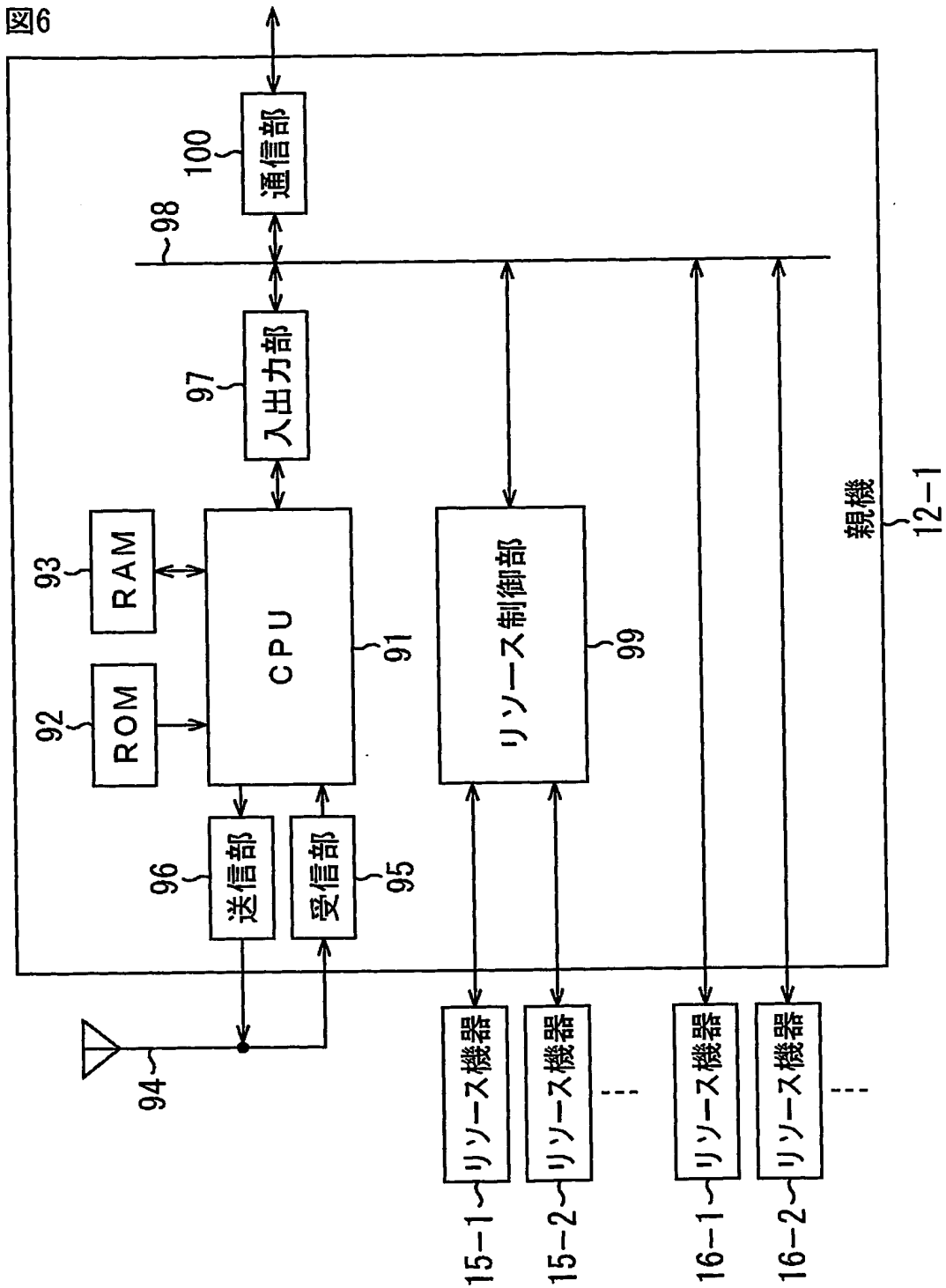
図5





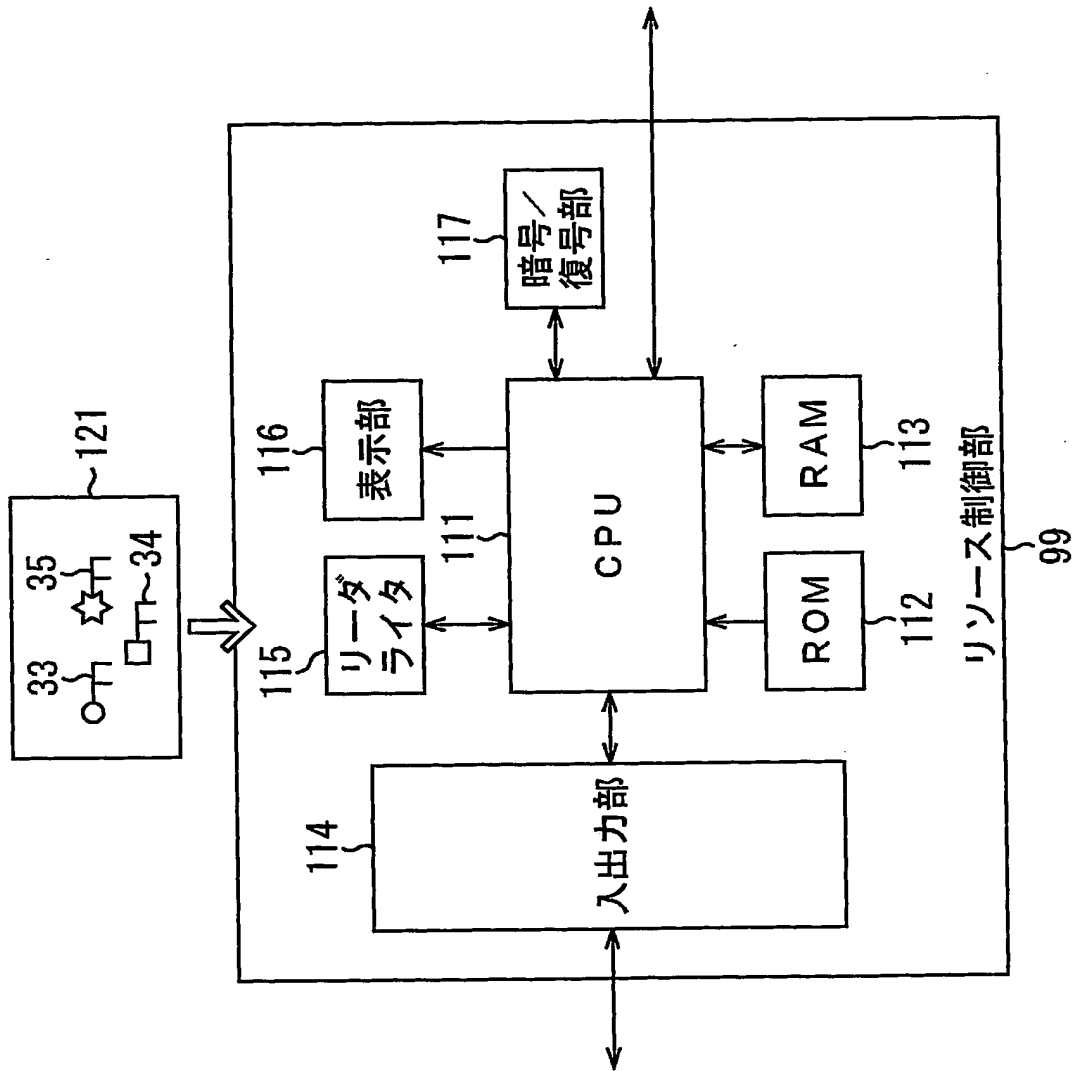
【図 6】

図6



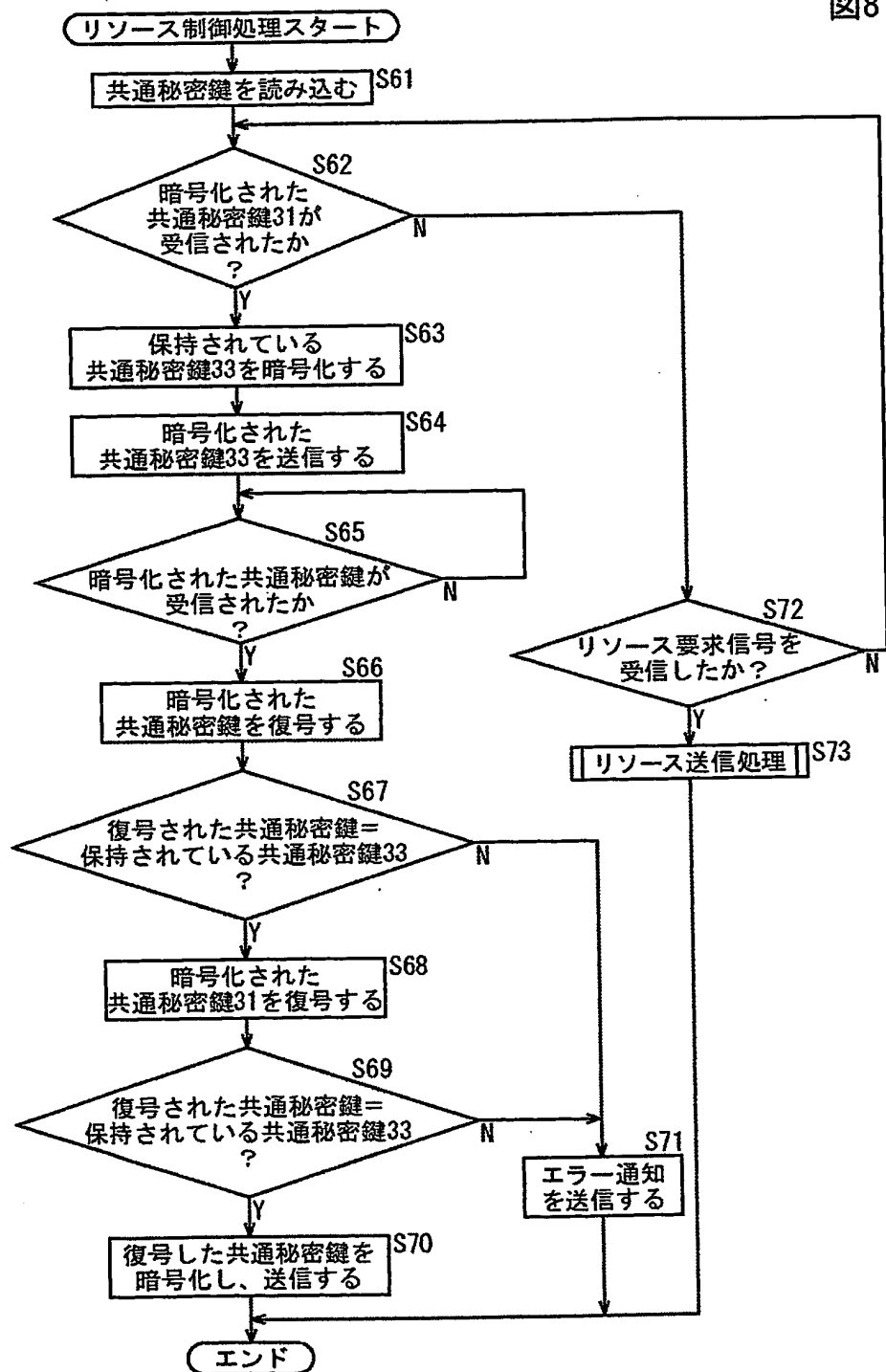
【図 7】

図7



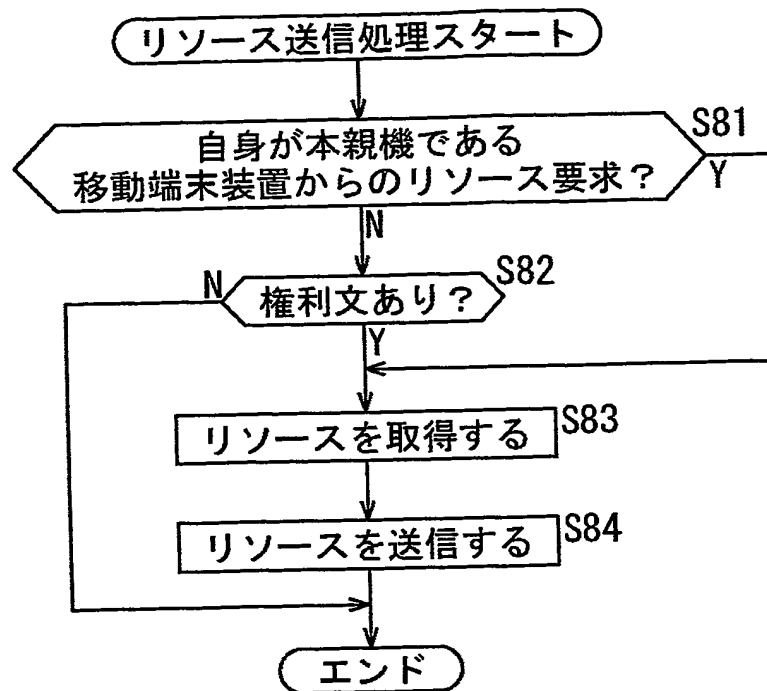
【図 8】

図8



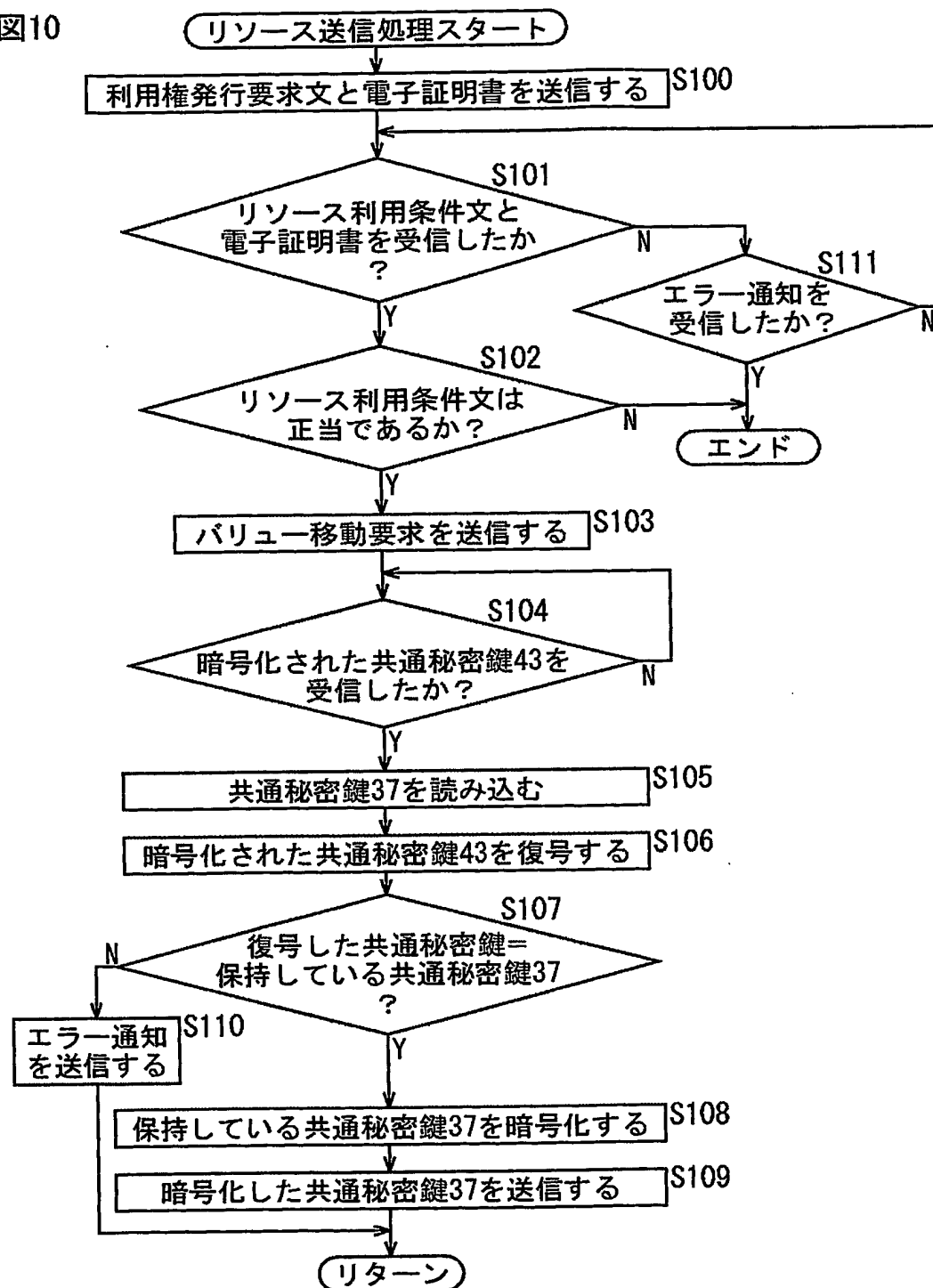
【図9】

図9



【図10】

図10



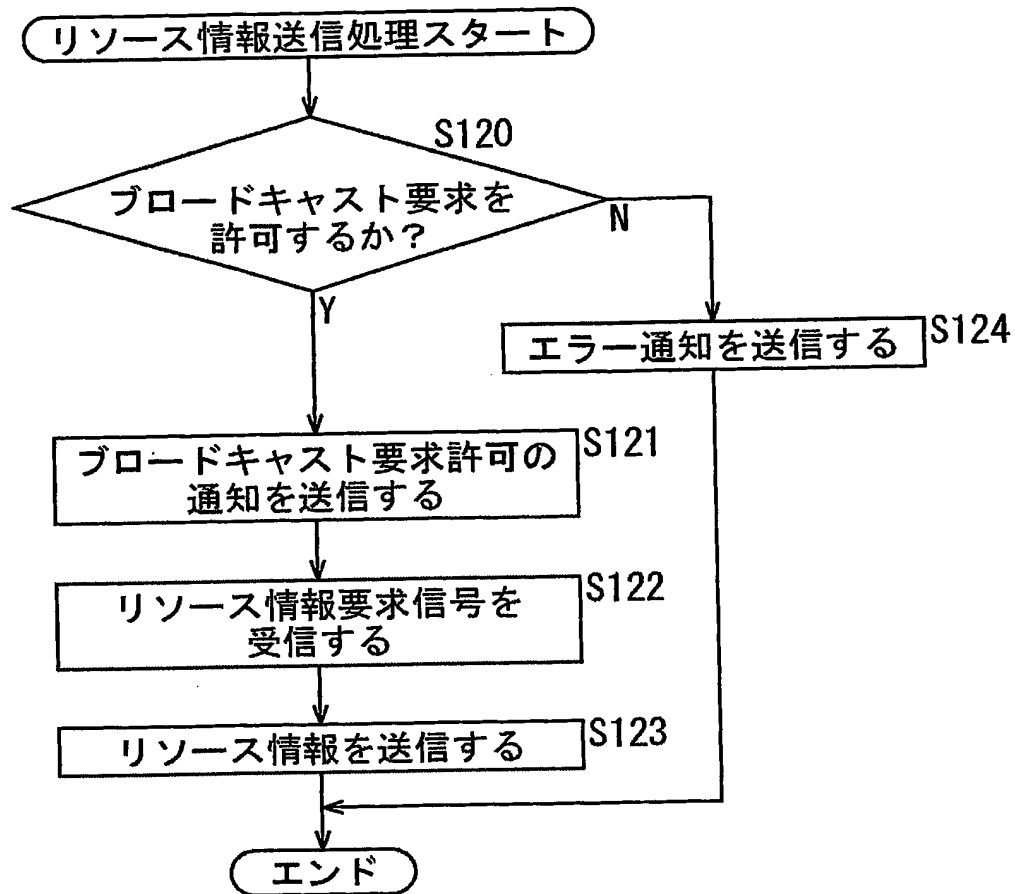
【図11】

図11

電子証明書
証明書のバージョン番号
証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
装置のID
装置の公開鍵

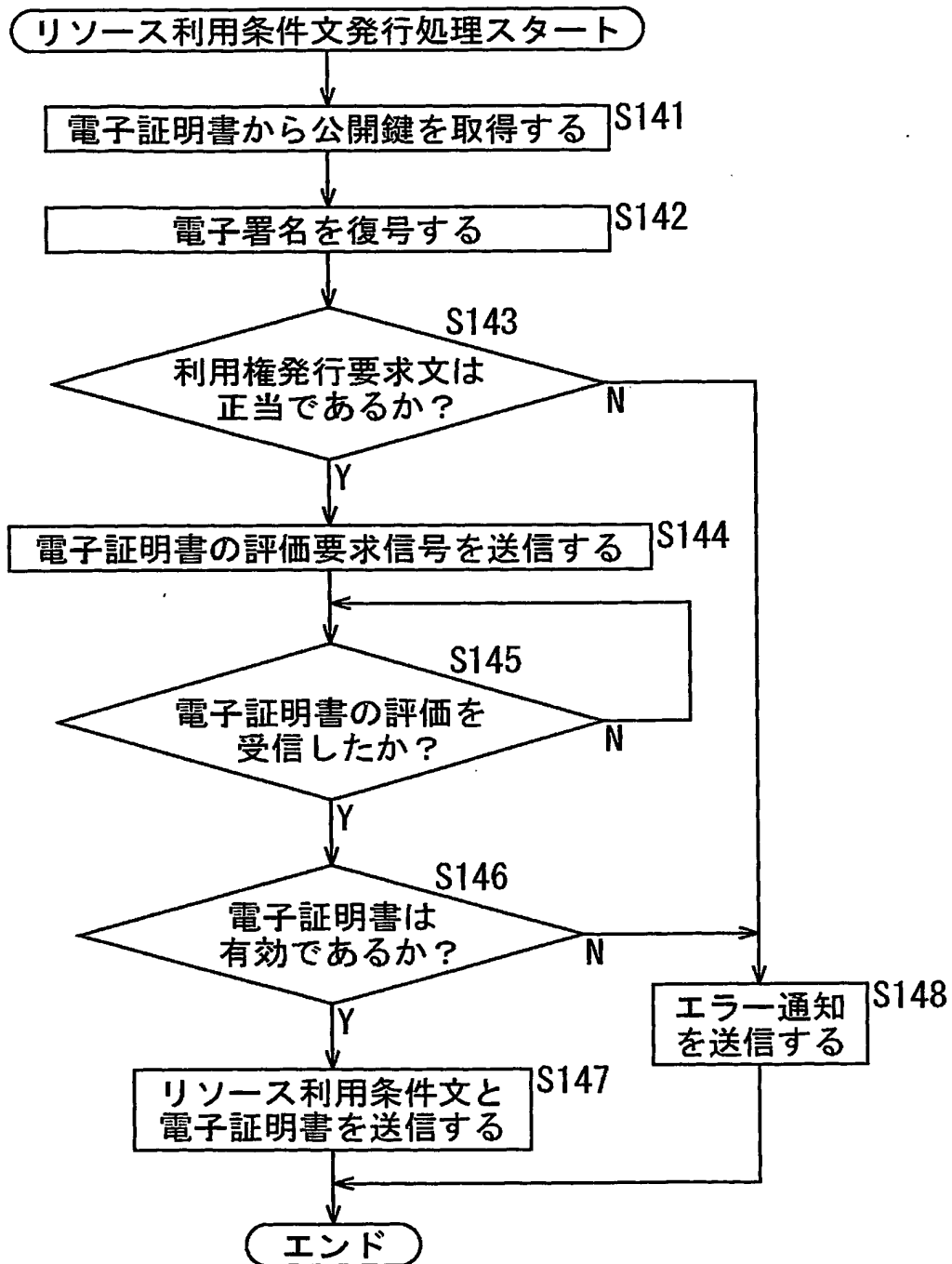
【図12】

図12



【図13】

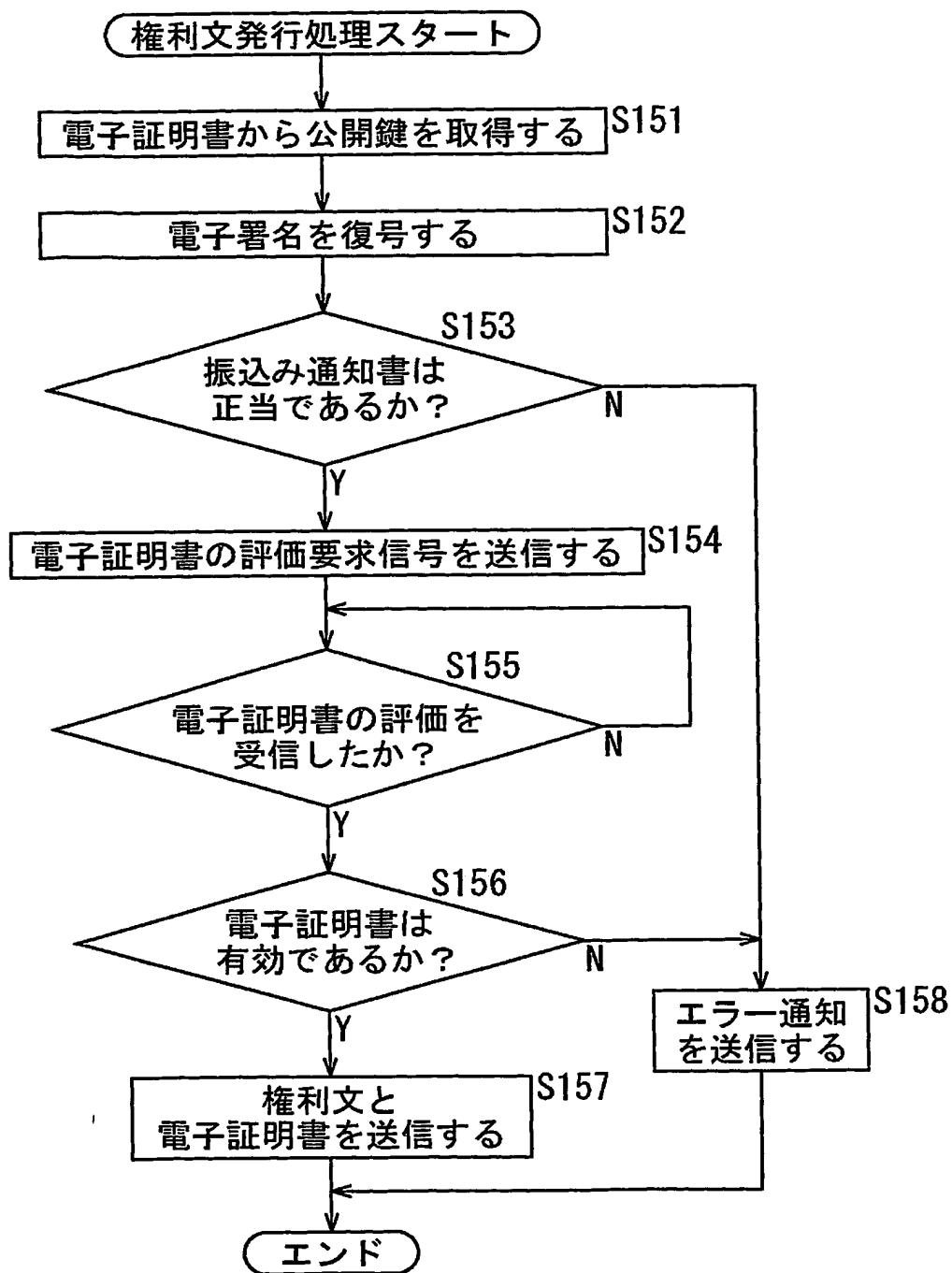
図13





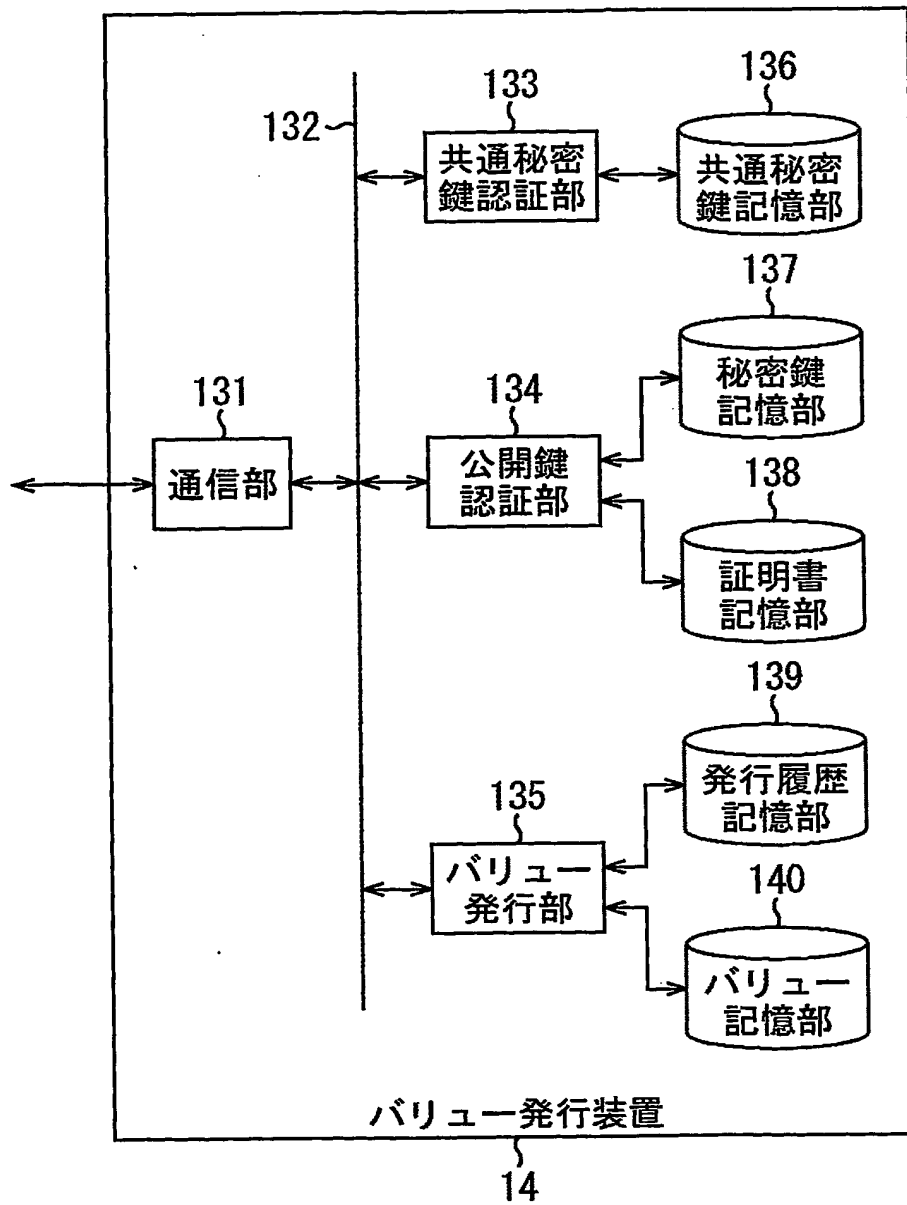
【図 14】

図14



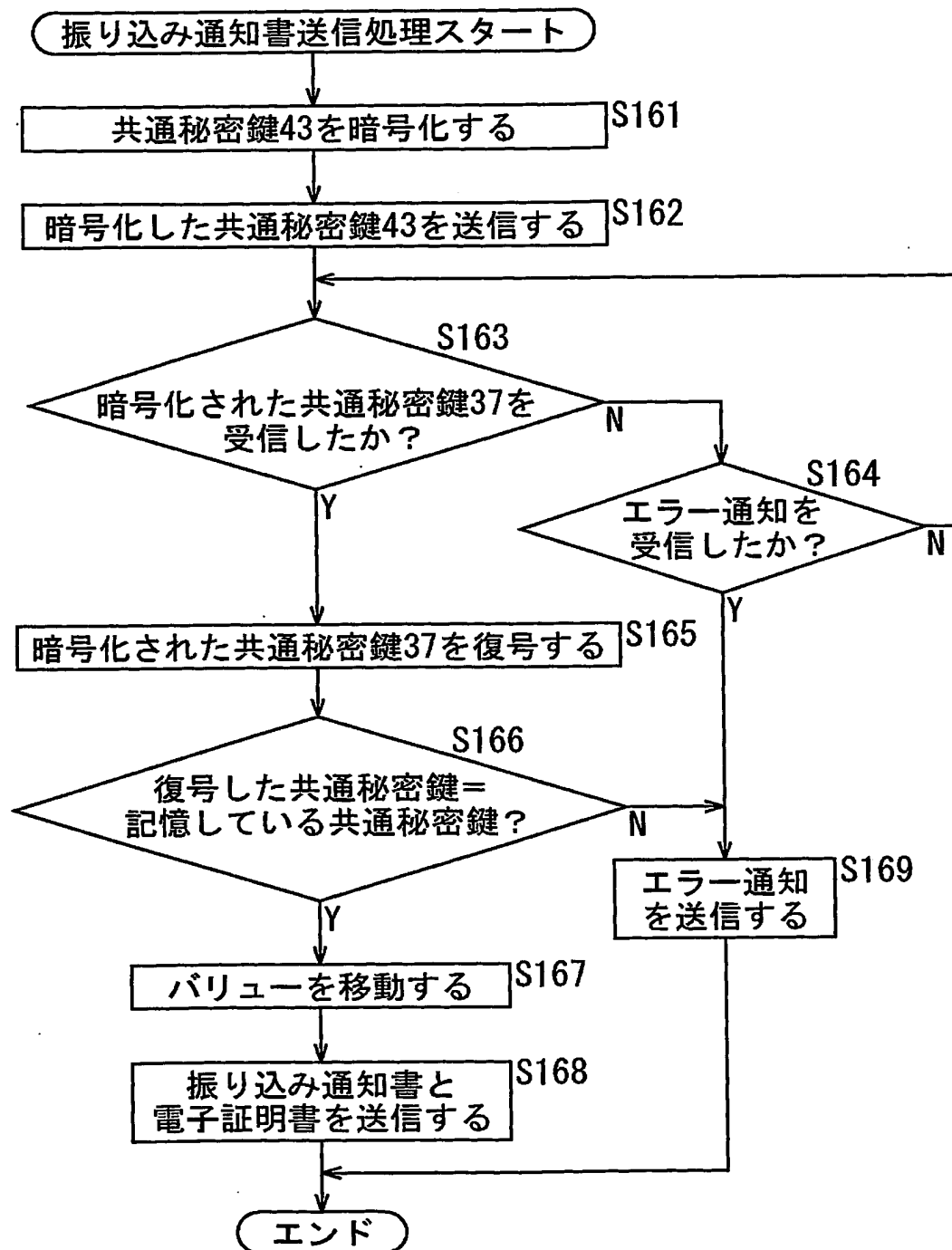
【図 15】

図15



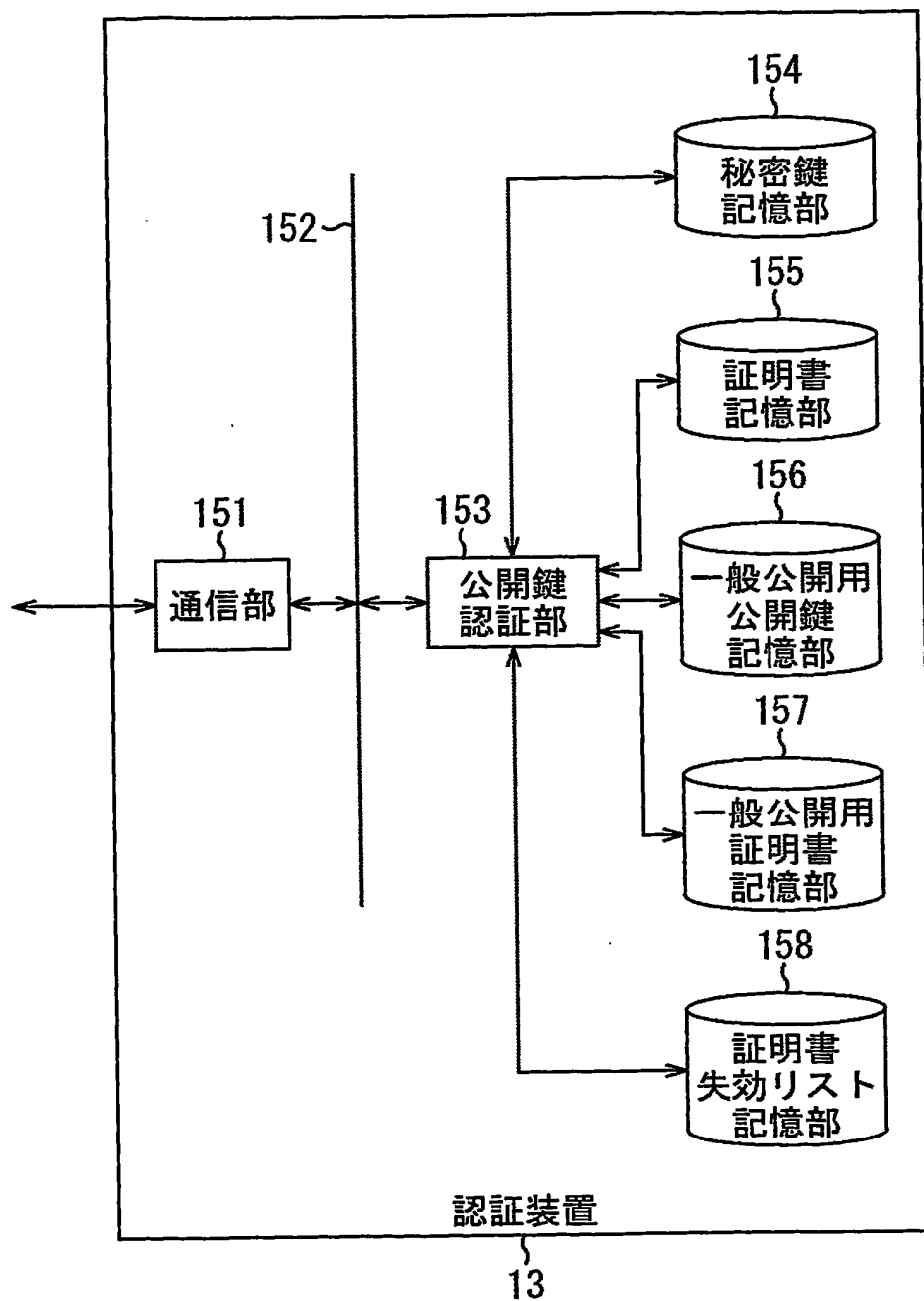
【図16】

図16



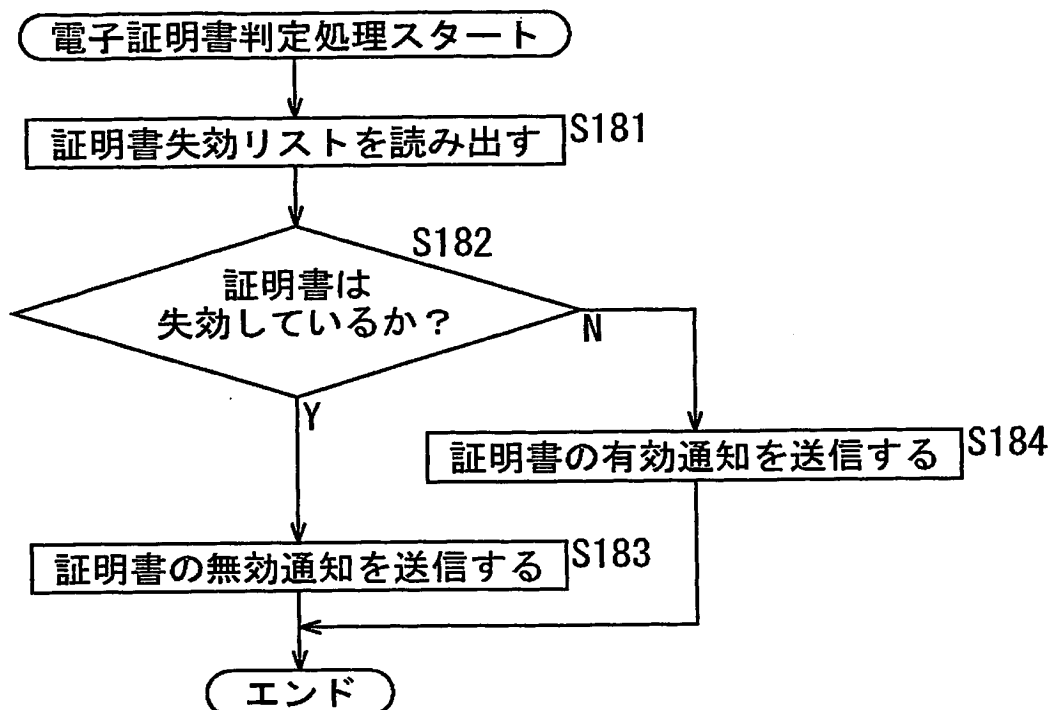
【図17】

図17



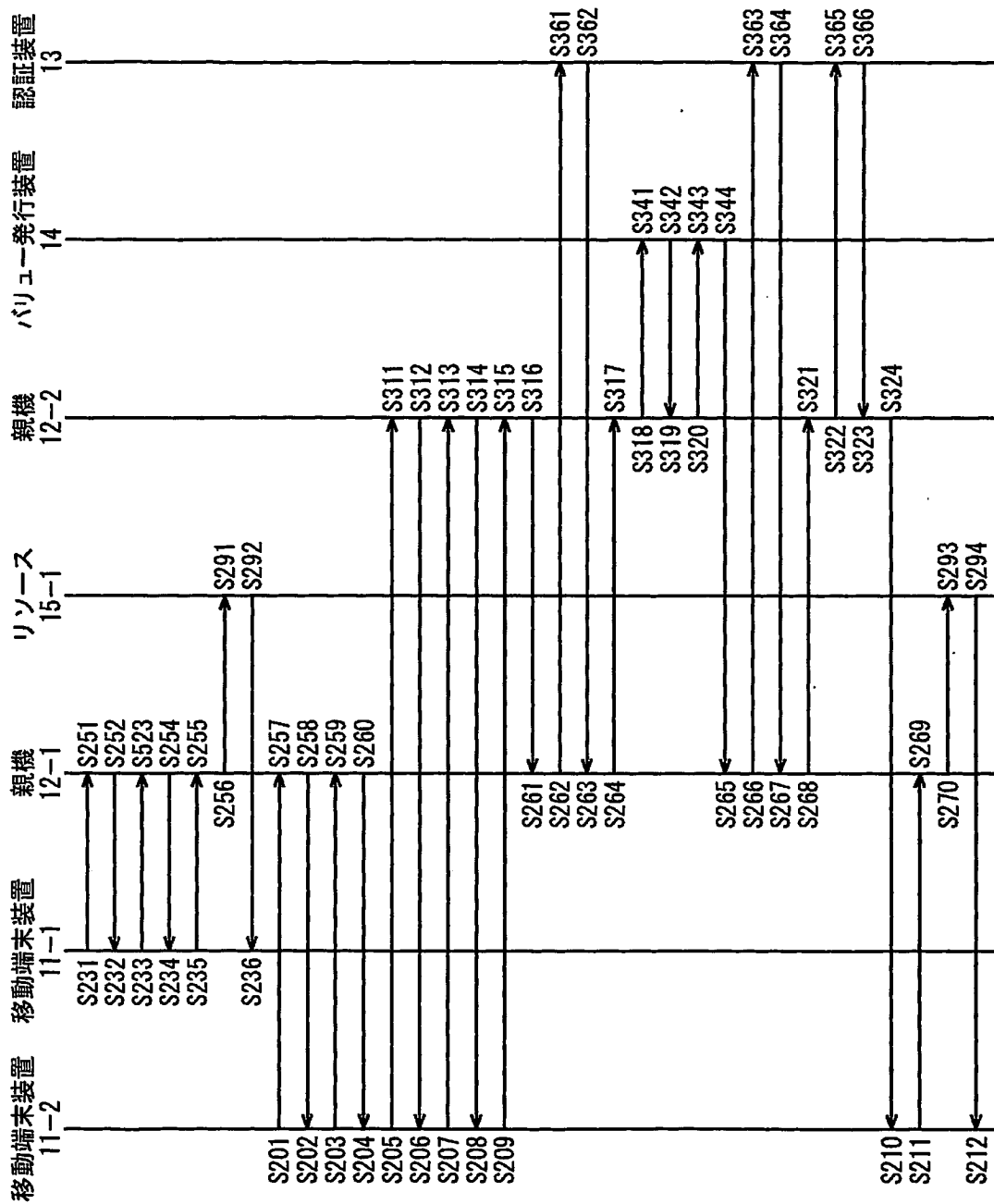
【図18】

図18



【図 19】

図 19



【書類名】 要約書

【要約】

【課題】 ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作することができるようにする。

【解決手段】 移動端末装置 11-2 は、親機 12-2 にリソース機器 15 のリソースを要求する。親機 12-2 は、親機 12-1 にリソース許可を要求し、親機 12-1 は、親機 12-2 に対してリソースを許可するために必要な対価を通知する。親機 12-2 は、バリュー発行装置 14 に対価の移動を要求する。バリュー発行装置 14 は、親機 12-2 の対価を親機 12-1 に移動し、振込み通知書を親機 12-1 に送信する。親機 12-1 は、その振込み通知書を受信し、リソース利用の権利を親機 12-2 を経由して移動端末装置 12-2 に与える。本発明は、無線通信システムに適用することができる。

【選択図】 図 1

特願 2003-092647

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住 所

東京都品川区北品川6丁目7番35号

氏 名

ソニー株式会社



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**